NETWORKING LAB

Total Periods	90	Maximum Marks	100 Marks
Lab. Periods:	6 Periods /week	Term Works	50 Marks
Examination	3hours	End Semester Examination	50Marks

LIST OF PRACTICALS:-

1. Introduction to Network
2. Discussion about the various type of network cable.
3. To study about the various topology
4. To study about different types of connectors in the network system.
5. Making of cross table and straight cable.
6. Installation of network interface card
7. To learn about IP address & configuring ip address.
8. Managing user accounts and parental control in window 7.
9. Managing user account in LINUX.
10. Sharing of Hardware Resources in the network.
11. To study the use of netstat & its options.
12. To study about ping command & its option.
13. To study about ipconfig commands &there options.
14. Connectivity trouble shooting using IP config & ping command
15. Installation of network operating system.
16. Configuring Network Operating System.
17. Create a simple network using CISCO packet tracer.
18. To study about switching & routing.
19. To study about Router &switch configuration.
20. To study about Router or Switch troubleshooting.
21. Lan Design Principles
22. To configure the primary WAN.
23. Configure IPv4 and IPv6 on a wireless access point.
24. Introduction to Network programming.
25. Basic Network Troubleshooting Commands.

Definition of Network:

Network is a group of interconnected computers which can exchange data between them.

There are basically three types of network

1) LAN (Local Area Network)
   LAN is a group of computers within a small geographical area i.e. an office building, a university campus.
   Data transfer speed can be maximum 1Gbps and LAN can have maximum 1000nodes. There are two types of LAN
   i) Peer to peer Network:
      In which all the nodes have the same role & there is no host computer.
   ii) Client Server Network:
      In which a host computer controls all the nodes called clients.

2) MAN (Metropolitan Area Network)
   MAN normally connects several LAN together using a switch as a router.
3) WAN (Wide Area Network)
   WAN connects multiple LANs or MANs across large geographical area using router.

Network Protocols:

Protocol is the set of rules that governs communication between computers in a network. They regulate the four characteristics of network.

➡ Objectives of protocol
- i) Access Method
- ii) Type of cables used
- iii) Physical Topology
- iv) Speed of data transmission

➡ There are five types of network protocol
- i) Ethernet
- ii) Local Talk
- iii) Token Ring
- iv) FDDI
- v) ATM

INDEX

Experiment:-1

AIM OF THE EXPERIMENT

Introduction to Network

STUDY OF NETWORK

a) Definition of Network:
Network is a group of interconnected computers which can exchange data between them.

b) Types of Network:
There are basically three types of network

4) LAN (Local Area Network)
LAN is a group of computers within a small geographical area i.e. an office building, a university campus.
Data transfer speed can be maximum 1Gbps and LAN can have maximum 1000nodes. There are two types of LAN

iii) Peer to peer Network:
In which all the nodes have the same role & there is no host computer.

iv) Client Server Network:
In which a host computer controls all the nodes called clients.

5) MAN (Metropolitan Area Network)
MAN normally connects several LAN together using a switch as a router.

6) WAN (Wide Area Network)
WAN connects multiple LANs or MANs across large geographical area using router.

c) Network Protocols:
Protocol is the set of rules that governs communication between computers in a network. They regulate the four characteristics of network.

⟹ Objectives of protocol

v) Access Method
vi) Type of cables used
vii) Physical Topology
viii) Speed of data transmission

⟹ There are five types of network protocol

vi) Ethernet
vii) Local Talk
viii) Token Ring
ix) FDDI
x) ATM

i) Ethernet:

- It is a network protocol which uses as access method called CSMA/CD(Carrier Sense Multiple Access/Collision Detection)
- In this protocol, each computer listens to the cable before sending anything on the network.

- If the network is clear the data packet is transmitted, otherwise if the network is busy(if some other system is already sending data), then the sender wait till the network is clear.
- If two systems attempt to send data at the same time both systems back off & wait for the random time to retransmit again.
- Used in bus, star, tree topologies.
- The type of network connection used are twisted cables, fibre optic cables etc.

ii) Local Talk:

- It is a network protocol developed for Apple, Machintosh.
- It also uses CSMA(Carrier Sense Multiple Access)/ CD(Collision Detection)
- The difference between local talk and Ethernet is any node that wants to transmit data first informs the network about its intent to send data before actually sending it.

iii) Token Ring:

- It is a network protocol developed by IBM.
- The access method used is token passing.
- The computers are so connected that the signal travels is a network in a logical ring.
- The computer which has electronic token is allowed to transmit dat.
- When a computer wants to send data, it can send only when it receives an empty token.
- The token gets transmitted through the network until it comes to a computer, which has data to send.
- The token ring protocol can only be used in a ring network using twisted cables or fibre optic cables.

iv) FDDI(Fibre Distributed Data Interface)

- It is a network protocol that is mostly used to interconnect two or more LANs over large distances.
- The access method used in token passing.
- FDDI normally is used in ring/star topology using fibre optic cables.

v) ATM(Asynchronous Transfer Mode)

- It is network protocol which transmits data in packets of fixed size unlike the other protocols.
- It also supports various types of media like video, audio & images.
- ATM is used in star topology using twisted cables or fibre optic cables.
- ATM is mostly employed by ISP (Internet Service Provider) to provide high speed internet.

d) Networking Devices:

i) Hub:

Network using star topology require a concentrator to accept all the cables from all the nodes. This concentrator is called a hub, which contain multiple independent parts that match the type of cable in the network. There are two types of hub

a) Passive Hub b) Active Hub

ii) Repeater:

Incoming signals may lose energy due to attenuation. A repeater is a device that amplifies the signal to counter-act the effects of attenuation.

iii) Switch:

Switch is a special type of hub which repeats incoming data packets only to the computer to which it is addressed.

iv) Bridge:

Bridge is a hardware device that is used to join two network segments together or to divide a large network into smaller segments. Bridge can connect network using different topologies. Bridge operates at the physical & data-link layer of OSI (Open Standard Interface) Model.

v) Router:

Routers are networking devices used to extend or divide network segments by forwarding data packets from one logical network to another. Routers work at the network level of OSI Model & connect TCP/IP host & LANs to the internet using leased lines.

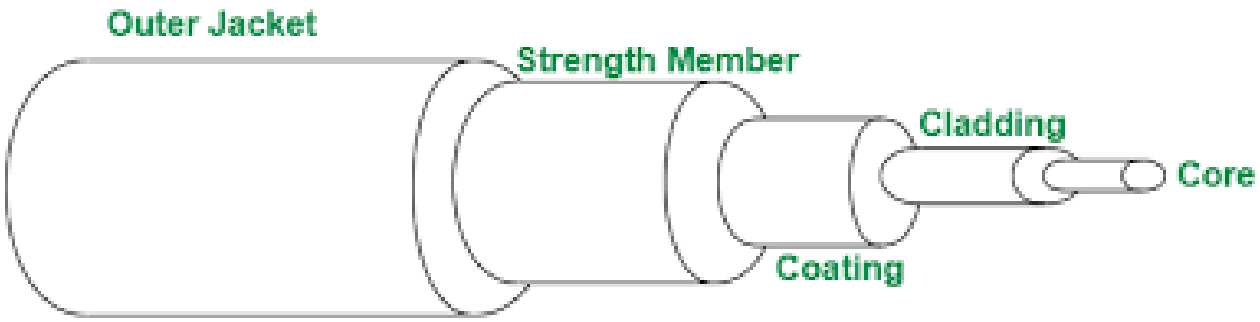
vi) Gateway:

Gateway is a network device used to connect network using different protocols.

To communicate with a host an another network the IP must be configured to the destination network. Gateway operates at network layer of OSI model.

vii) NIC (Network Interface Card):

NIC is a hardware installed on a computer so that it can communicate with the internet.



OPTICAL FIBER CABLE

Experiment :-2

AIM OF THE EXPERIMENT

Discussion about the various type of network cable.

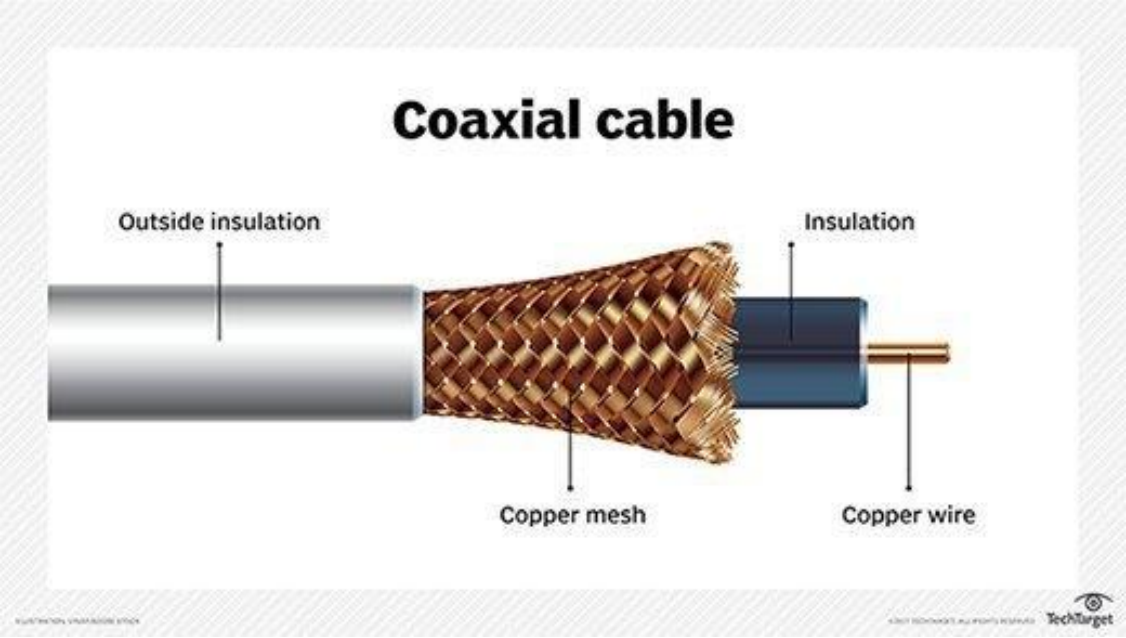
DESCRIPTION

There are 4 types of Network cable.

i. Unshilded Twisted Pair (UTP) cable-are broadly used in the telecommunications and computer industries as Ethernet cables & telephone wires. In a VIP cable, conductors forming a single circuit is circuited and twisted around one other to cancel out electromagnetic interference (EMI) from external source.

ii. Shilded twisted pair (STP) cables-
Ofter optics cables possess a center glass as simply Ethernet cables, STP cables employ a special type of copper business wires . In a UTP cable conductor forming a single circuit An external shiledfuncation is a ground added to the started twisted pair of telephone wires .
Shileded twisted pair cable can an area with potential interference and risk to an unshiled twisted pair cable can also help to expand the distance between the cables.

iii. FibreOptics :-
Fibre optics is also known as Optical fibre .
Avantages :-
Its speed is 100 Gbps use for long distance transmission and communication .
Secure & very low signal .
Extemally high throughput.
Corression& water nesistant .



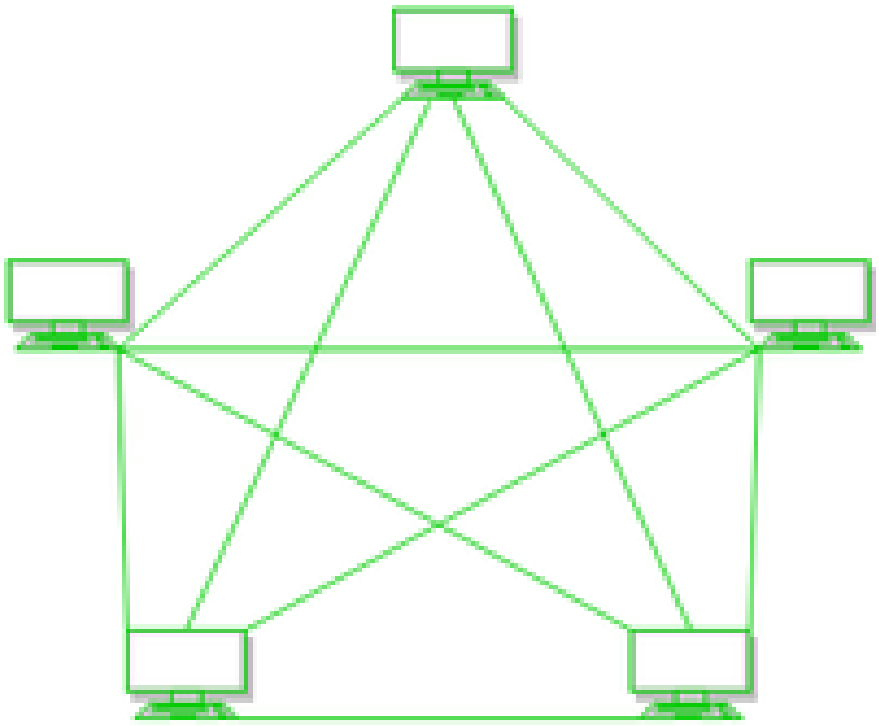
Disadvantage –
More expensive than co-axial cables & twisted cable Difficult to install and modify.
Maintenance is also high.
Co-axial Cable-
Its speed is above 10 Gbps
It is used for video transfer, television, telephone lines and LANs.
Single solid copper wire are covered by insulating material carries both analog & digital
Co-axial carries high frequency rang signal two types:-
i) Thick net ii) thin net.

Disadvantage-

More expensive than twisted pair & not compatible with that.

CONCLUSION-

The above experiment has done by me successfully.



MESH TOPOLOGY

Experiment :-3

AIM OF THE EXPERIMENT

To study about the various topology

TOPOLOGY:-

Geometric representation of how the computers are connected to each other is known as topology. There are five types of topology-Mesh, Star, Bus , Ring & Hybrid.

TYPE OF TOPOLOGY:-

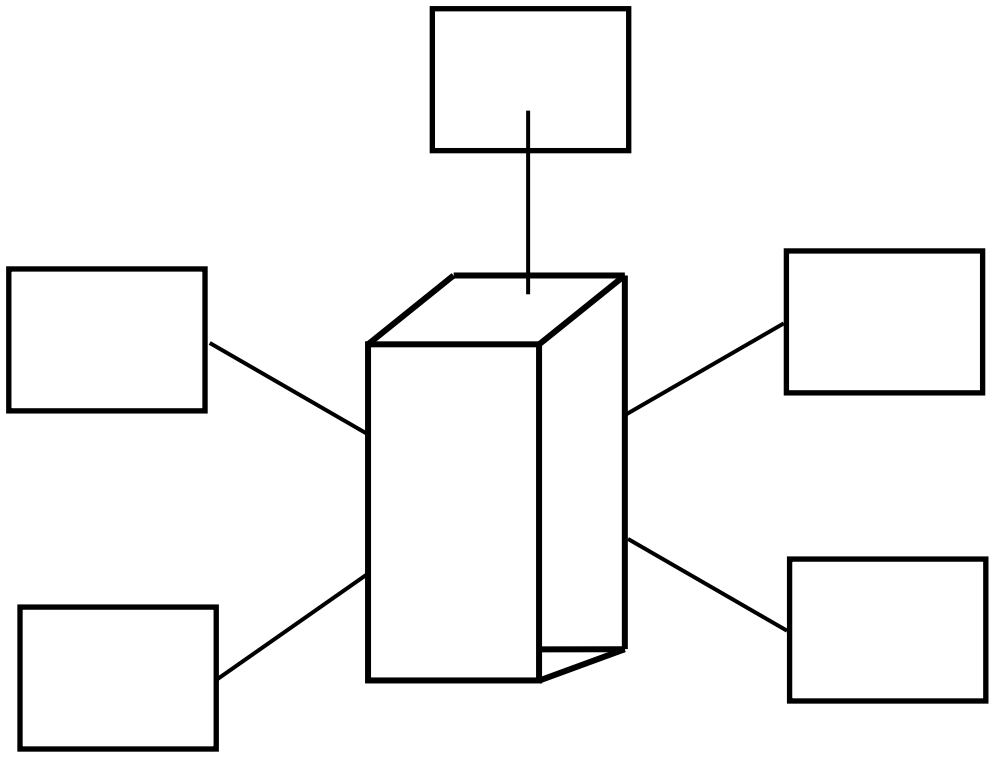
There are 5 types of topologies in computer network.

1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology

Mesh Topology:-

In mesh topology each device is connected to every other device on the network through a dedicated cable

- It means that the link only carries data for the two connected devices only.
- Let's say we have n devices in the network, then each device must be connected with (n-1) devices of the network.
- Number of links in a Mesh topology of n devices would be n (n-1)/2.



STAR TOPOLOGY

ADVANTAGES OF Mesh Topology:-

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable robust, as failure of one link doesn't effect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

DISADVANTAGES OF Mesh Topology:-

1. Amount of wires required to connect each system is tedious & headache.
2. Since each device needs to be connected with other devices,
   Number of i/o ports required must be huge.
3. Scalability issues because a device can't be connected with large number of devices with a dedicated point to point link.

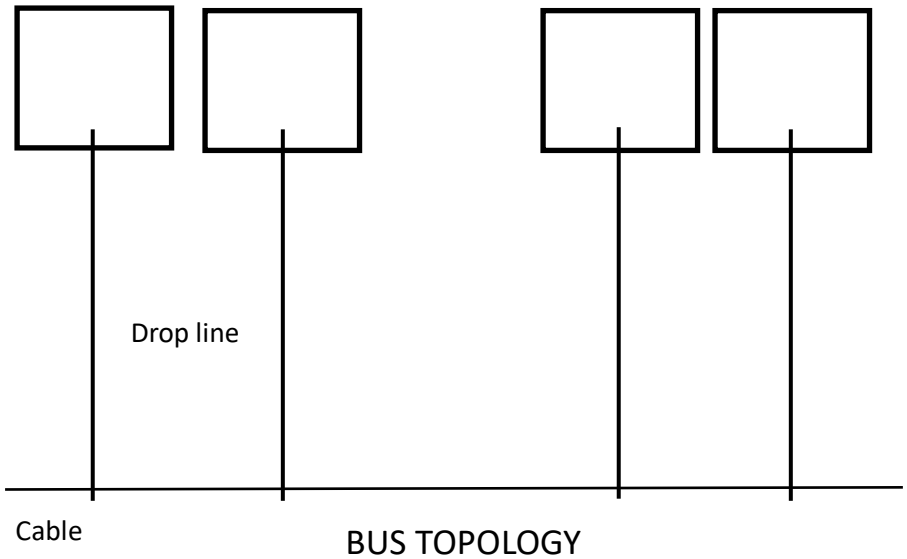
STAR TOPOLOGY:-

In star topology , each device in the network is connected to a central device called Hub.

Unlike Mesh Topology, Star topology doesn't allow direct communication between devices.

A device must have to communicate through hub.

If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.



BUS TOPOLOGY

ADVANTAGE OF STAR TOPOLOGY:-

1. Less expensive because each device require only one I/O port and needs to be connected with one link.
2. Easier to install.
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust , if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

DISADVANTAGES OF STAR TOPOLOGY:-

1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

BUS TOPOLOGY:-

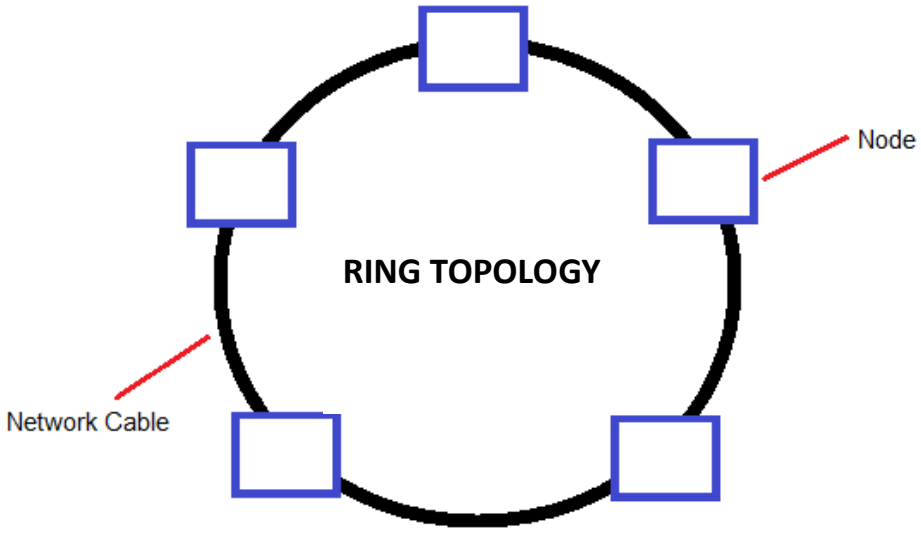
In BUS Topology, there is a main cable and all devices are connected to the main cable through drop down lines.

There is a device called tap that connects the drop down line to the main cable.

Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

ADVANTAGES OF BUS TOPOLOGY:-

1. Easy installation, each cable need to connected with backbone cable.
2. Less cables required than mesh & star topology.



DISADVANTAGE OF BUS TOPOLOGY:-

Difficult in fault detection.

Not scalable as there is a limit of how many nodes you connect with backbone cable.

RING TOPOLOGY:-

In ring topology each device is connected with two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it.

This structure from a ring thus it is known as Ring Topology.

If a device want to send data to another device then it sends the data in one direction, each device in topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

ADVANTAGES OF RING TOPOLOGY:-

1. Easy to install
2. Managing is easier as to add or remove a device from the topology required to be changed.

DISADVANTAGES OF RING TOPOLOGY:-

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

HYBRID TOPOLOGY:-

A combination of two or more topology is known as hybrid topology . for ex:-A combination of star & mesh topology known as hybrid topology.

ADVANTAGES OF HYBRID TOPOLOGY:-

We can choose the topology based on the requirement . for ex, Scalability is our concern then we can use star topology instead of bus topology.

DISADVANTAGES OF HYBRID TOPOLOGY:-

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

Experiment :-4

AIM OF THE EXPERIMENT

To study about different types of connectors in the network system.

Description:-

There are different types of network cable connectors are used in network system.

They are-

a) RJ-45(Registered Jack)
b) RJ-11(Registered Jack)
c) SC ST(Subscriber Connector & Stright Tip)
d) BNC(Bayonet Neill-Concelman Connector)

RJ-45(Registered Jack)

- The “RJ” in RJ45 stands for “Registered Jack” since it is a standardized networking interface. The ‘45’ simply refers to the number of the interface standards.
- Each RJ45 connector has light pins, which means an RJ-45 cable contains eight separate wires.
- An ethernet cable,the eight wires within it which are of different colors, from those four wires are of soild colors while other four are stripped.
- RJ45 is primarily used to connect devices over an Ethernet connections.
- RJ45 can be wired in twidiffernetways .i.e T-568A & T-568B.
- These wiring standards are listed below-

T-568A

1. White/Green(Receive+)
2. Green(Receive-)
3. White/Orange
4. Blue
5. White/Blue
6. Orange(Transmit)
7. White/Brown
8. Brown

T-568B

1. White/Orange(Transmit)
2. Orange(Transmit)
3. White/Green(Recevie+)
4. Blue
5. White/Blue
6. Green(Receive-)
7. White/Brown
8. Brown

RJ11(Registered Jack)

- It is standard telephone cable connector and has 4 slots.
- RJ-11 is the acronym for registered jack-11,a four or six-wire connector.

- RJ-11 is the 'telephone' standard. If you still have a wired land line phone, it almost has one RJ-11 phone jack or a cord with an RJ-11 connector attached to it.

SC ST(Standard/Subscribe connector and Straight Tip)

- Fiber network segments always reqire two fiber cables: one for transmitting data & one for receiving data.
- Each end of fiber cable is fitted with a plug that can be inserted into a network adapter, hub or switch.
- A straight tip connector(ST Connector) is a connector used in fiber optics cables that utilize a bayonet style plug & socket.
- It has become the defector standard for commercial wiring. The ST connector allows unidirectional communication. So two ST connectors and two fiber cable are used for bidirectional communication.

BNC Connector-

- The Bayonet Neill –ConcelmanConnector(BNC Connector) is a type of coaxial radio frequency(RF) electrical connector that is used in place of Coaxial connectors.

Experiment :-5

AIM OF THE EXPERIMENT:-

Making of cross table and straight cable.

DESCRIPITION:-

What is straight through cable?

A straight through cable is a type of twisted pair cable used in local area networks to connect a computer network hub such as a router. These types of cable is called a potch cable and alternative to wireless connections where one or more computer access a router through a wireless signal. Straight through cable use one wiring standard. Both ends use T568A wiring standard or both ends use T568B wiring standard.

What is crossover cable?

A crossover Ethernet cable is a type of Ethernet cable that used to connect computing devices together directly unlike straight through cable, the RJ45 crossover cable uses two difficult wiring standard one end uses another end uses T568B wiring standard two devices of some type two computers of two swikles to each other.

RIQUIREMENT:-

- Unshielded twisted pair cable (UTP)
- Modular connector (Spscplug,aka RJ45)
- Criping tool
- Cable tester

There are 4pairs of wires in an Ethernet cable and an Ethernet connector(spsc) has eight pin slots. Each pin is identified by a number, starting from left to right, with the clip facing away from us. The two standards for waiting Ethernet cables are T568A & T568B. T568B is the most common & is what we will be using for our straight Ethernet cable. The cable bellow show the proper wired to the pins.

T568A Standards :-

Pin 1- White/Green

Pin 2- Green

Pin 3-White/Orange

Pin 4-Blue

Pin 5-White/Blue

Pin 6-Orange

Pin 7-White/Brown

Pin 8-Brown

T568B Standards :-

Pin 1-White/Orange

Pin 2-Orange

Pin 3-White/Green

Pin 4-Blue

Pin 5-White/Blue

Pin 6-Green

Pin 7-White/Brown

Pin 8-Brown

- STEP 1-Strip the cable jacket about 1.5 inch down from the end.
- STEP 2-Shread the four pairs of twisted wire a part for cost. You can use the pull string to strip the jacket further down it you need to then out the pull string out it down if you need to ,then cut the pull string cat6 cable have a spine that will also need to be cut.
- STEP 3-Untwisted the wire pare & neatly align them the T568B orientation . Be sure not to untwist them any further down the cable than where the jacket begins ,we want to leave as much of the cable twisted as possible.
- STEP 4-Cut the wires and straight as possible, about 0.5inch above the end of jacket.
- STEP 5-Carefully insert the wires all the way into modular connector, making sure that each wire passes through the appropriate guides inside the connector.
- STEP 6- Push the connector inside the crimping tool 8 squeze the crimper all the way down.
- STEP 7- Repeat step 1-6 for other end of cable.
- STEP 8- To make sure you have successfully terminated each end of the cable use a cable tester to test each pin. When we are all done, the connector should look like this.
- CONCLUSION:- The above experiment has been done by me successfully.
  - A BNC connector connects various radio frequencies up to 2GHz and voltage under 500V DC and is used in electronic architecture such as audio, video and networking.
  - One of the benefits of the BNC connector is its close fitting connection. The connection is locked by the BNC male connector main conducting wire.
  - It is secured in the place with an external ring that turns to a locked positions.
  - BNC is also used in high grade analog communication test equipment due to its low signal loss architecture. Coaxial Ethernet cabling is nearly always terminated with BNC connectors

<u>Conclusion</u>

From the above experiment we concluded that the Experiment has successfully done by me

Experiment :-6

AIM OF THE EXPERIMENT

Installation of network interface card

Apparatus Required

1) NTC
2) Diver CD
3) LAN

Network interface card(NIC) Installation:-

Short for network interface card,a NIC is also commonly referred to as a network adaptor and is an expansion card that enables a computer to connect to a network such as a network such as a home network and /or the internet using a etheme cables with RJ45 connector .This section discuss the process of installing a network interface card/network interface card /Network adapter.

INSTALLATION PROCESS IN WINDOWS:-

1) First step is to read the user's guide &familiarize yourself wih the new card.
2) Power down pc remove the AC power card.
3) Open the computer case.
4) Find an available peripheral component interconnect (PCI)slot on the motherboard & remove slot insert of one exits.
5) Carefully remove the network card from it's static proof plastic envelope & slide into the slot.
6) Seal the card in the slot firmly with gentle pressure along the length of the card, especially the slot itself.
7) Close the computer case.
8) Click start, then click control panel.
9) In category view click performance then click 'system' icon and then the hardware lab.
10) Click the network adapter and manage button.
11) Beneath , it should appear the name of your Ethernet if the text in the 'device status' box says "This device is working properly" then you successfully installed the card & are finished.
12) If the next in the "Device status" box doesn't says "This device is working properly" then write down on a peace of paper and continue next step.
13) Click the trouble shoot button and follow installation double click you followed the directions above install the most up to data device drives.

Experiment :-7

AIM OF THE EXPERIMENT

To learn about IP address & configuring ip address.

EXPERRIMENT –

CLASS OF IP ADDRESS:-

Internet Protocol hierarchy contains several classes of IP address to be used efficiently in various situations as per the requirement of host per network.

Broadly the IPV4 addressing system is divided into five classes of IP addressing. Internet corporation for assigned names & numbers is responsible for assigning IP address. The octal referred here is the left most of all. Decimal notation of IP address .

1^{st} octet	2^{nd} octet	3^{rd} octet	4^{th} octet
11000000	101010000	00000001	10011000
192	168	1	152

Number of network = 2^n network – bits.

Number of hosts/network = 2^n host bits -2

CLASS A ADDRESS:-

The first bit of the first octet is always set to 0(Zero)

Thus the first octet ranges from 1-127 i.e

00000001 - 01111111

The defult subnet mask for class A IP address is 255.0.0.0 which implies that class A IP address can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2). Class A IP address format is thus ONNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

CLASS B ADDRESS :-

An IP address which belongs to class B has the first two bits in the first octet set to 10 i.e

10000000-10111111

128-191

Class B has 16384 (2^{14}) Network address & 65534 (2^{16} – 2) host address.

Class B has IP address format - 10NNNNNN.NNNNNNNNN.HHHHHHHH>HHHHHHHH.

CLASS C ADDRESS :-

The first octet of class C IP address has its first 3 bits set to 110, that is –

11000000-11011111

192 – 223

Class C IP address range from 192.0.0.X to 223.225.225.X. class C IP address format is 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH.

CLASS D ADDRESS:-

Very first four bits of 1st octel in class D IP address are set to 1110, giving the range of

11100000 – 11101111

224 – 239

Class D has IP address range from 224.0.0.0 to 239.225.225.225. class D is reserved for Multitasking. In Multitasking data is not destined for particular host that is why there is no need to extract host address from the IP Address, and class D doesn't have any subnet mask.

CLASS E ADDRESS:-

This IP class is reserved for experimental purpose only for R & D or study IP address in this class range from 24.0.0.0 to 225.225.225.254 like class D.

STEP FOR CONFIGURING CLASS ADDRESS:-

A static IP Address is useful for hosting servers or websites and for sharing large files. To set a static IP address in window 7,8 and 10;

1. Click <start menu >control panel>Network & sharing center
2. Click change adapter settings.
3. Right click on wi-fi or location are connector.
4. Click properties and select internal protocol version 4.
5. Click properties and following IP address.
6. Select use the following IP address.
7. Enter the IP address , subnet mask , default gateway.
8. Click ok.
9. Your computer displays a static IP address.

CONCLUSION:-

From the above experiment we study about IP address, configuring IP address.

Experiment :-8

AIM OF THE EXPERIMENT

Managing user accounts and parental control in window 7.

EXPERIMENTAL OBSERVATIONS :-

To go to your user accounts

STEPS:-

1.Go to the control panel from the start menu.

2.Click add or remove user accounts.

3.Getting to your user accounts.

4.The manage accounts panel will appear, you will see all of the user accounts here or manage existing ones.

5.The manage accounts panel.

6.To create a new account.

7.From the manage accounts panel, click create a new account.

8.Type an account name.

9.creating an account.

10.Select standard user or administrator.

11.Click create account.

12.Changing an account's settings.

To create a password :-

STEPS :-

1.From the manage accounts pane, click the account name.

2.Edit an account.

3.Click create a password.

4.Create a password.

5.Type a password in the new password field, and it in the confirm new password field.

6.Type a password and hint.

7.If you want, you can type a password hint to help you remember your password.

8.Click create password.

9.To go back to manage accounts pane, click manage another account.

10.Account passwords are case-sensitive which means capital and lowercase are treated as different characters.

To change account pic:-

Steps-

1.You can also change the picture for any account. This picture appears next to the account. This picture appears to the account more name & helps you easily identify the account.

2.From manage account pane, click the account name or picture.

3.Click on change the picture.

4.Change the picture.

5.Select a picture or click browse for more pictures.

6.To select on of your own.

7.Account pictures.

8.Click change picture.

To set up parental controls :-

1.Go to the control panel from the start menu.

2.Click set up parental controls for any user.

3.Getting to parental controls.

4.Click on any standard account.

5.Choose an account.

6.Click on to turn parental controls on.

7.Parental controls main page.

8.Now you can click time limits, games or allow and block specific programs to set the parental controls. We will explore each of these on the next page.

9.To learn more about available parental control options you can use, checkout this article on five free ways to protect your hides online.

CONCLUSION :-

You can now create new accounts whenever you want and all users will be able to easily access their own files and customize the appearance of window 7 while they’re logged into their respective accounts.

Experiment :-9

AIM OF THE EXPERIMENT

Managing user account in LINUX.

Experimental Observation:

Linux is a multi-user OS. There is a high need of an administrator, who can manage user accounts, their rights & the overall system security for user management in LINUX.

1. Creating a user
2. Deleting disabling account
3. Adding users to the usergroups
4. Finger
5. Linux, Unix user management commands.

1. OS using Linux USER Commands. Next in this Linux user command Next in this Linux admin tutorial, we will learn how to create a user in Linux Administration.
   The steps for creating a users are: Using terminal,
   Step 1- Use command sudo add user.
   Step 2- Enter password for the new account and confirm
   Step 3- Enter details of the new user and press 4
   New account is created using GUI.
   Step 1- Go to the system settings look for an icon which says 'User accounts' .
   Step 2- Click on the unlock icon & enter a password when prompted, then click the plus sign.
   Step 3- A new window would pop up, asking you for adding information to the new user account. The account type offers two choices stand and administrator. Administrations can do things like add and delete users, install software and drivers. Fill in the full name, user name, click on create.
   Step 4- The new account would show, but would be disabled by default.
   To activate it, click the password option and add a new password. Click change to enable the account.

2. Deleting, disabling account
   Terminal
   for disabling an account using terminal remove the password set o the account.
   Sudo password- 1 'User name'.

3. To delete an account, use the command.
   Sudo userdel-r 'user name'.
   Using GUI
   1) Highlight the user account and click the minus sign to delete.
   2) For disabling click on the area where the password is stored, and you would get the following prompt. Select disable this account. Groupmode "press Tab key twice".
   3) New to add a user to a group .
      Syntax-
      Sudo usermode- a.GGroundname username

4) Removing a user from usergroup
   Sudo decauser user Groupname
   The GUI Method
   If you do not want to run the Linux User Commands in terminal to manage users and groups, then you can install a GUI add-on.
   Sudo apt-get install gonme-system tools, once done, type users-admin.
   Appear-
   The syntax ‘Finger’ gives data on all the logged users.
   The syntax ‘Finger username’ specifies the information.

   LINUX/UNIX User Management Commands:
   1) Sudo adduser username
   2) Sudo passed -1 ‘username’
   3) Sudo userdel-r ‘(username)’. Delete a user.
   4) Sudo deluser user Groupname
      Remove user from a usergroup.
      Finger
      Gives information on all logged in the finger username.
      Gives information of a particular user.

      CONCLUSION-
      You can use both GUI or terminal for user administration in LINUX user management. You can create , disable and remove user accounts using LINUX admin commands. You can add/ delete a user to a usergroup.

Experiment :-10

AIM OF THE EXPERIMENT

Sharing of Hardware Resources in the network.

Experimental observation-

Printers-

Network printers can be configured as shared devices so that others on the network can use them. If you are using window 7 go to start device and printers. Window displays the properties dialog box for the selected printer. Click the share this printer check box & optionally. If checked then all the processing required prior to querying the print job occurs on the client computer. If unchecked the computer hosting (serving) the printer does the processing for all print jobs sent through it, when you are done sharing the printer. Click OK to close the printer's properties dialog box. In order to access the shared printers from a different system, go to that system and if the system, choose start. If the system is using window 8 or window 10 display the control panel and clock view devices and printer then click view devices and printers and click the add printer option. The windows to system will perform a search for a device or printer to this PC. Windows display the find a printer by other options section of the 4th option. If you are using window 10 and the system immediately starts scanning the network for available printers. The network printer is added to the computer's list of available printers.

FILE, FOLDERS AND DISK DRIVES

File folder and entire disks can also be shared among network connected system, and the procedure is similar to that of sharing a printer. Using window explorer, night click the folder you want to share with others on the network and select share with specific people (window 7) or share specific people (window 8). If you are using window to, display File explorer and make sure that share tab of the ribbon is displayed. Then Right click the folder you want to share with others on the network & select give access to specific people. Window then displayed the Network Access dialog box. You can then optionally changed the share name, when ready to share, click on OK to finish the process.

CONCLUSION-

From the above we learnt about resources sharing over a network.

Experiment :-11

AIM OF THE EXPERIMENT

To study the use of netstat & its options.

Introduction:-

Windows dose have a netstat command and it can come handy when you are in need of network related monitoring and troubleshoot.

Requirement of Netstat Command:-

Consider you have any of the following requirement . How to find who or which process owns the port in window server.

To make sure the port is open from DS to data base from window server etc. Netstat command.

Windows have the following syntax and option support.

1) Find all the 'established' and 'waiting' TCP connection.

2) Get details into of TCP and DCP connection.

3) List of connections and ports open with process.

Information - Find who runs the port.

4) Find who view the port with port with process ID and process name.

5) Get fully qualified remote address on the open connection.

6) How to Grip for a specific port with windows netstat command.

7)Execute windows netstat command in internal.

Netstat Command Options:-

To Find all the established any waiting for TCP connections This is a simple netstat command it would result the simple list of TCP connections established on server.

1) netstat – To get detailed info on ports open, ports listening, connection established for TCP/UDT connections.

2) netstat – a command would give the extended result of ports opened on the server and established connection.

3) netstat-an:-

Show what is the difference between netstat-a & netstat-an.

Why the latter one is faster, simply put, netstat – an command would only show the remote server IP address.

4) Netstat-ab:- If you don't want the domain name be displayed in the foreign address and on with the numeric ID information , adding an n-option makes the command, faster. You can use netstat-and as said earlier.

5) Get the process Id and process name of the ports and communication open. In the example , with destat-ab, use were any getting the process name who owns the port, not the process ID.

6) netstat-abo:-Netstat window command. Using f-option to get fully qualified domain names (FQDN) or Remote address. You can use option to get fully qualified remote address.

7) netstat-afb:-You can't use –n with-f is as one with compromise the other. The option -f is for FQDN where -n is for any numeric. Look for a specific part or process id using find STP. The windows netstat command output is so large and it you are looking for a pressure port or process or PID.

8)netstat-afb:-Findstar SCSC in the proceeding snapshot you can see that findstar was used to check if port 8080 is open and listening.

9) netstat-abo &Findstar8080:- here the interval is 5 seconds. The netstat –abo command would run every 5 second with CTRL+C.

Various other windows,Netstat Commands & their usages:-

Netstat has more to offer and here we have listed some of command snippets & their usage as quick list. Display Routing table.

Netstar-r

Display only UDP connections –netstat –abpudp –ab

Display only TCP connections

Netstat -abp.tecp –ab

CONCLUSION-

We studied about various netstat commands.

Experiment :-12

AIM OF THE EXPERIMENT

To study about ping command & its option.

Introduction:-

To ping command is a command prompt command used to test the ability of the source computer to reach a specified destination computer .it's usually used as a simple way to verify that a computer can communicate.

Experiment:-

The ping command operated by sending internet control message protocol , Echo request manage to the destination computer & waiting for a response .How many of these response are returned , that the ping command provides .Ex-you might find that there are no response when pinging a network printer or maybe you need to ping a router to verify that your computer can connect to it, to eliminate it possible came for a networking issue.

Ping Command Syntax:-

-t :- Using this option will ping the target until you force it to stop by using ctrl+c.

-a :- This option will revolve , if possible the host name of an IP address target.

-n count :- this option sets the number of ICMP Echo request to send from 1 to 4294967293. The ping command will send a 32-byte echo request if you don't use the –l option .

-f :- Use this option to prevent ICMP Echo from being fragmented by routers between you & the target.

-v :- This option allows you to set a type of service (TOS)value. Beginning in window7,this option no longer functions but still exist for compatibility reasons.

-r count :- Use this option to specify the number of hope between your computer & the target computer. Hence that you would like to be recorded &displayed . the maximum value for count is 9,so use of fracert command instead ,if you are interested in viewing all between two device.

-s count :- Use this option to report the time ,in internet time stamp format that each echo request is received & echo reply is sent. Meaning that only that 1st four hopes can be time stamped.

-w :- Without specifying a timeout value when executing the ping command adjust the amount of time in mili seconds that ping waits for each reply. If you don't use the –w option ,the default timeout value of 4000 is used ,Which is 4 seconds.

-R :- This option tense the ping command to trace the round trip path.

-S seraddr :- use this option to specify the source address & -p use ping a hyper-v network virtualization provider address.

-4 :- if force the ping command to use IPVA only necessary if target is a host name & not an IP address.

-6 :-this process the ping command to use IPV6 only but as with the -4 option ,is only necessary when pinging a host name, target .This is the destination you wish to ping, either an IP address or a host name.

Ping command option:-

Ping[-t][-a][-n count][size][-f][-1TTL][-v Tus][-r count][-8 count][-w timeout][-R][-S][-P][-4][-6] target[12]. The availability of certain ping command sluitches& other ping command syntax might differ from OS to OS. If you are not sure how to interrupt the ping command syntax, use the help of switch with the ping command to show detailed help about the commands several option. IPv4 address is not used in-R & -s option , they work only with IPv6.

Conclusion:-

From the above experiment we studied about ping command & their options.

Experiment :-13

AIM OF THE EXPERIMENT

To study about ipconfig commands &there options.

Experiment-

IPCONFIG command

Configure (IP (Internet protocol configuration)

Syntax:- IPCONFIG/all-Display feels configuration inform

IPCONFIG/all-Display feels configuration.

IPCONFIG/release (adapter)-Release the Ip address for the specified adapter.

IPCONFIG/Ausdrs - purge the DNS revolver cache.

IPCONFIG/register dns-refresh all DHCP leases & re-register DNS names.

IPCONFIG/display dns-display the contains of the DNS revolver cache.

IPCONFIG/show classic adapter-Display all the DHCP class ids allowed for adapter.

IPCONFIC/select a lid adapter-(classid)-Modify the chop classid if adapter name contains space, use `Adapter Name'

The default is to display only the IP addresses subnet mask & default gateway for each adapter bound To TCP/IP, for release & renew It has no adapter name specified, the IP address leases for all adapter bounce. To TCP/IP will be released is specified, then the classid is revolved .

Ex:-

- Ipconfig . . . .show information
- Ipconfig/all. . . . show detailed information
- Ipconfig/renew. . . .renew all adapters
- Ipconfig/renew EL.. . .renew any connection that has its name starting with EL.
- Ipconfig/release*con*. . . .release all machingconnectins

  Ex-local area connection 1/"local area connection2"
- Ipconfig/select classid "Local area connection TEXT. . .set the DHCP class ID for the named adapter to=TEST

Experiment :-14

AIM OF THE EXPERIMENT

Connectivity trouble shooting using IP config & ping command

DESCRIPTION:-

If a network having problem, you can use the special command line in window 7 to test a TCP/IP installation .The following are 3 most commonly used commands.

IPCONFIG:-

Use to determine if a network configuration has been initialized & if an IP address & valid subnet mask are, the configuration initialized & there are no duplicates for IP address. If a subnet mask of 0.0.0.0 is returned, the IP address is a duplicate.

HOSTNAME:-

Used to determine the computer name of the local computer.

PING:-

Used to query either the local or another computer on the network to see whether it respond.

TO TEST NETWORK CONNECTION:-

- Click start, click all programs, click accessories & click command prompt. From the command prompt window displayed type. ipcontig& press enter. The IP address & subnet mask of the current computer should be returned. If this didn't happen, there is a problem with the current configuration.
- Type-host name & press enter. The computer name of the local computer should be returned.
- Type : ping followed by the name of another computer on your network& press enter. You should get 4 replies from the other computer.
- If ping didn't work with a remote computer try it on the current computer by typing: ping 127.0.0.1 & Press Enter. Again you should get4 replies, this time from the current computer i.e your workstation.
- If you didn't get reply here, you have a problem with either the network set up or the NIC. If you did get a reply here, but not in the above step (on remote computer then there is a problem either in other computer or in the cable & devices connect them.
- Close the command prompt window.

Experiment :-15

AIM OF THE EXPERIMENT:-

Installation of network operating system.

Requirement-

Network OS CD.

Experiment-

Installation over the network.

Normally you install the NOS directly from the CD-ROM distribution dises on the server's CD-ROM drive. However you can also install the OS form a shared device located on another computer provided that the server computer already has access to the network .You can either use a shared CD-ROM drive or you can copy the entire contents of the distribution CD ROM dise on to a shared hard disk drive obviously the server computer must have network access in order for this technique to work. If the server already has an OS installed it probably already has access to the network. It not you can install NOS on both the computer from a floppy that has basic network support.

If you're going to install the NOS onto more than one server, you can save time by first copying the distribution CD onto a shared hard drive that's because even the fasted CD-ROM drives are slower than the network .Even with a basic 10Mbps network access to hard drive data over the network is much faster than access to a local CD-ROM drive. Automated & remote installations.

In case you find yourself in the inevitable position of installing a NOS onto several servers you can use a few tricks to streamline the process.

1) Automated setup lets you create a setup script that provides answers to all the questions asked by the installation program. Creating the setup script is a bit of work so automated setup makes sense only if you have more than a few servers to install.
2) Microsoft has a feature called remote installation services (RIS) that lets you install windows server version from a remote network location without even going to server computer .This is a trickly to set up. However, so it's really worth if only if you have a lot of servers on which to install operating system.(You can also RIS to install client OS)

Conclusion-

We have successfully installed the NOS.

Experiment :-16

AIM OF THE EXPERIMENT

Configuring Network Operating System.

NETWORK CONFIGURATION PROCEDURE:-

Network Software initialisation takes place along with the initialisation of the OS Software .

PARAMETERS SUPPLIED DURING NETWORK CONFIGURATION:-

- IP address of each network interface on every machine .
- Host names of each machine on the network . You can type the host name in a localfile or a name service database.
- NIS, NIS+ or DNS domain name in which the machines resides of applicable .
- Default router addresses.Yousuuply this only if you have a simple network topology with only one routers attached to each network or your routers don't run routing protocols such as the Router Discovery Server Protocols(RDSP) or the Router Information Protocal(RIP).
- Subnet Mask(required only for networks with subnets)

CONFIGURE A HOST FOR LOCAL FILE MODE:-

Use this procedure for configuring TCP/IP on a machine that runs in local files mode.

1. Become superuser and changed to the /etc directory.
2. Type the host name of the machine in file /etc/nodename.
   ex-if the name of the host is tenere type tenere in the file.
3. Create a file name
   /etc/host name.interface for each network interface
   (The soloris installation program automatically creats this file for the primary network interface)*not required.
4. Type either the interface IP address or interface name in each /etc/hostname.interface file.
   e.g-create a file named hostname. Ie1,&type either the IP address of the host interface or the host name.
5. Edit the /etc/inet/hosts file to add IP address
6. Type the host's fully qualified domain name in the /etc/default domain file.
   E.g-suppose host tenere was part of domain deserts. World wide.com,type same in /etc/default domain.
7. Type the router's name in /etc/default router.
8. Type the name of the default router and it's IP address etc/inet/hosts
9. If your network each subnetted ,type the network number. & the netmask in file /etc/inet/netmasks.
   If you have set up a NIS or NIS+ sever ,you can type net mask inform in the appropriate database on the server as long as server and clients are on the same network.
10. Reboot each machine on the network.

SETUP A NETWORK CONFIGURATION SERVER:-

1. Become superuser and change to root directory of the prospective network configuration server .
2. Turn on the in.tftpd daemon by creating the directory/ tftpboot . #mkdir/tftpboot.
   This configures the machine as a TFTP,bootparams and RARP sever.
3. Create a symbolic link to directory. #ln-s /tftboot /tftpboot /lftboot.
4. Enable the tftp line in intetd.conf. check that the /etc/inetd.conf entry reads: tftpdgramudp wait root/usr/sbin/in.tflpdin.tftpd-s/tftpboot.
   This prevents intftpd() from retrieving any file other than one located in/tftpboot.
5. Edit the host database, and add the host names and IP address for every client on the network.
6. Edit the others database , and add create entries for every host on the network to run in network client mode.
7. Edit the bootprograms database.
8. Reboot the server.

CONFIGURING NETWORK CLIENTS:-

Network clients receive their configuration information from network configuration server. Therefore, before configuring a host as a network client you must ensure that at least one network configuration server is set up for the network.

CONFIGURE HOST FOR NETWORK CLIENT MODE:-

1. Become superuser.
2. Check the directory for the existence of an/etc/node name file. If one exists,delete it.
3. Create the file/ect/hostname.interface,if it does not exist make sure that the file is empty.
4. Ensure that the /etc/inet/hosts file contains only the host name and IP address of the loopback network interface.
5. Check the existence of an/etc/default domain file. If one exists, delete it.
6. Ensure that the search paths in the client's /etc/nsswitch.conf reflects the name service requirements for your network.

SPECIFY A ROUTER FOR THE NETWORK CLIENT:-

1. If you have only one router on the network configuration and you want the network configuration server to specify it's name automatically, ensure that the network client does not have a /etc/ default router file.
2. To override the name of default router provided by the network configuration server create/etc/defaultrouter, type hostname and IP address and add them to clients/etc/inet/host.
3. If you have multiple routers on the network, create/etc/default router on network client, but leave it empty. If the system discovers that routers are not responding to RDISC protocol, it uses RIT & runs the daemon in.routed to keep track of them.

Experiment :-17

AIM OF THE EXPERIMENT

Create a simple network using CISCO packet tracer.

How to create a Network in CISCO Packet Tracer:-

In packet tracer, you can add a Router, Switch & PC to the working environment to create a basic network & examine how data communication takes place between computers.

Follow the steps below to examine how computers on two segments (2 different LANs) connected to the Cisco Router on Packet Tracer Communicate.

Step-1:-Add one Cisco Router, 2 Cisco Switches & 4PCs on the program's workspace . Then note the port & slot numbers of the router's Gigabit-Ethernet interfaces in the workspace. Double click on the router to open the IOS command interface.

Step-2:-In the CISCO router CLI window, assign on IP address to the Gigabit Ethernet 0/0 interface & execute the no shutdown command to activate the interface.

Step-3:-After configuring Gigabit Ethernet 0/0 interface the port will be green. The meaning of this color is; the interface is activated /active & working.

Step-4:- To assign an IP address to the Gigabit Ethernet 0/1 interface is activate the port perform following commands:

Router (config) #

Router (config) # interface Gigabit Ethernet 0/1.

Router (config-if) # ip address 192.168.2.1 255.255.255.0.

Router (config-if) #no shutdown

Router (config-if) #

% LINK-5-CHANGED: Interface Gigabit Ethernet 0/1, changed state to up.

%LINKPROTO-5-UPDOWN: Line Protocol on Interface Gigabit Ethernet 0/1, changed state to up.

Router (config-if) # end

Router #

%SYS-5-CONFIG_I: configured from console by console.

Router#

Step-5:-Now,you can see that router's Gigabit Ethernet ports are connected to the switches & are active.

Step-6:- Now you need to assign an IP address to the computers that you add to the computers that you add to the topology. To do this, click on the PC to which you will assign an IP &on the desktop tab, Click IP configuration.

Then you need to address the PC account to the IP block of the network on which the network is. Account to the topology above , assign an IP address from Block 192.168.1.0/24 as PCO is connected to the network under the router's Gig0/0 interface.

Configure the IP address, subnet mask & default gateway settings for PCO as in the following

DHCP= static , IP address =192.168.1.10

Subnet mask = 255.255.255.0, Default Gateway = 192.168.1.1,

DNS server =<Blank.

Step-7:- Click Command prompt on PCO,& then ping the CISCO Router Gig0/0 default gateway to test the network connection .

Step-8:- This time, configure the TCP/IP settings of PC3 on the 192.168.2.0/24 network as follows.

DHCP=Static, IP Address =192.168.2.1, DNS Server =<BLANK>

Step-9:- When you ping the Gigabit Ethernet 0/1 interface (default gateway) via PC3,you can see that the operation was successful.

Step-10:- Likewise, if you ping the Router's Gigabit Ethernet 0/1 interface via PCO, the operation will still be successful because one of Router's main task is to help the different networks connected on it to communicate with each other.

Step-11:-Ping operation to PC2 computer with IP address 192.168.2.10 via PCO;

Step-12:-Ping operation to PC2 computer with IP address 192.168.2.20 via PCO;

Step-13:-You can examine the MAC address of computers when you execute the show arp command at the Cisco CLI Command Prompt.

Experiment :-18

AIM OF THE EXPERIMENT

To study about switching & routing.

SWITCHING:

- When a user access the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information for one computer network to another network is known as switching.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computer together which one local area network.
- Network switches operate at 2nd layer in OSI model.
- Switching is transparent to the user & doesn't require any configuration in the home network.
- Switches are use to forward the packets based on MAC address.
- A switch is used to transfer the data only to the device that has been address. It verifies the destination address to route the packets appropriately.
- It is operate in full duplex mode.
- Packet collision is minimum as it directly communicates between source & destination.
- It doesn't broadcast the message as it works with limited bandwidth.

ADVANTAGES:

- Switch increases the bandwidth of the network.
- It reduces the only workload on individual PCs as it sends the information to only that device which has been address.
- It increases the overall performances of the network by reducing the traffic of the network.
- There will be less farm collision as switch creates the collision domain for each connection.

DISADVANTAGES:

- A switch is more expensive than network bridges.
- A switch cannot determine the network connectivity issues easily.
- Proper designing & configuration of the switch are required to handle multicast packets.

ROUTING;

- Routing is process of selecting path along which the data can be transferred for source to the destination. Routing is performed by a special device known as a router.
- A router works at the network layer in the OSI model and internet layer in TCP/IP model.

- The routing algorithm are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

TYPES OF ROUTING:

Routing can be classified into three categories-

- Static routing
- Default routing
- Dynamic routing

STATIC ROUTING :

- It is also known as non-adaptive routing.
- In this the administrator manually
- Adds the router routes in the routing table.

ADVANTAGES:

- It has no overhead on the CPU usage of the router.
- It has no bandwidth usage between the routers.
- Provides security as only administrator is allowed to have control over the routing to a particular network.

DISADVANTAGES:

- For a large network, it's difficult to add is route manually to the routing table.
- The system administrator should have good knowledge of the topology.

DEFAULT ROUTING:

- It is a technique in which a router is configured to send all the packets to the same hop device & it doesn't matter whether it belong to a particular network or not. A packet is transmitted to the device for which it is configured in default routing.
- It is used when network deal with the single exit point.

DYNAMIC ROUTING:

- Also known as adaptive routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition of topology of network.
- Dynamic protocol are used to discover the new router to reach the destination.

ADVANTAGES:

- It is easier to configure.
- It is more effective in selecting the best route to the changes in the condition or topology.

DISADVANTAGES:

- It is expensive of CPU & bandwidth usage and is less secure than other types of routing.

Experiment :-19

AIM OF THE EXPERIMENT

To study about Router &switch configuration.

Switch configuration:

The switch is a network device that is used to segment the networks into different subnetwork called subnets or LAN segments. It is responsible for filtering & forwarding the packets between LAN segments based on the MAC address.

Steps to configure the switch:

Step1: Open the packet tracer using desktop icon & take a switch (PT_switch) from the devices.

Step2: Configure the host name of the switch 0.

- Click on switch 0 & go to command line Interface.
- Then change the host name to “sh”.

Command: switch>

switch >en

switch #conf t

switch (config) #hostname sh

sh(config) exit.

Step3: Set a message of the day (MOTD) banner for the users.

Command: sh(config) #banner motd $

- Then, emter MOTD & end it with ‘S’ to exit .

Step 4: Set up line control password & enable secret password.

Commands: sh#conf t

sh(config)#

sh(config)#line con o

sh(config-line) #password GFG123

sh(config-line)#login

sh(config-line)#exit

sh(config)#enable secret GFG@123

sh(config)#exit

Step 5: Verify the password.

- When you try to login first, it will ask for the link control password.
- The to configure the terminal it will ask to enable a secret password .
- Command: sh # copy run startup-config
  The above end is used to save the configuration.

Router configuration:

Routing is the method of selecting a path for network packet over the internet or between or through multiple networks. Routing is conducted on many kinds of

networks, such as public switched telephone network (PSTN) & computer networks such as the Internet.

Steps to Configure the Router:-

Step 1: Open the packet tracer using desktop icon & take a Router (2911) & PCO from the devices.

- Connect the router o with the PCO with the help of a console cable
- Then, click on PCO & go to the terminal &type y.
- Finally, we can configure the router with the help of a PC.

Step 2: Configure the Host name of the router 0.

- Click on PCO & go to the terminal
- Then change the host nam to “r1”

Command – router>

router >en

router #conf t

router (config) # hostname r1

r1 (config) exit

Step 3: Set a message of the day (MOTD) banner for the users .

Command : r1(config) # banner motd $

Then , enter MOTD & end it with ‘s’ to exit .

r1(config) # banner motd S

Enter text message. End with the character ‘$’.

Unauthorized access is strictly prohibited $.

Step 4: Setting up line control password & enable secret password.

Commands:- r1#conf t

r1(config)#
r1(config)#line con o

r1(config-line)#password GFG123

r1(config-line)#login

r1(config-line)exit

r1(config-line)#enable password cisco

r1(config)#enable secret GFG@123

r1(config)#service password-encryption

sh(config)#exit

*Step5:-*Verifying password.

When you try to login first, it will ask for the line control password.

- Then to configure the terminal it will ask to enable a secret password.

The above end is used to save the configuration.

Command:-r1# copy run startup-config

Experiment :-20

AIM OF THE EXPERIMENT

To study about Router or Switch troubleshooting.

Router &Switch Troubleshooting

Review the following troubleshooting issues that may occur with routers/switches.

- A switching loop that is not blocked via (STP) results in data that be forwarded.
- Bad/ improper cables connected to a switch or router may result in a bad link, incapable of transmitting data.
- Ports & interfaces that are incorrectly configured are incapable are in capable of transmitting data.
- Switches that have ports configured as VLANs should be assigned correctly in order for the system/ host on those VLANs to communicate.
- A power failure will result in bringing a network down unit power can be restored via electric generator or restoration of service.
- A router with a bad / missing route can result in delayed or non-delivery of data.
- Mismatched MTU & MUT black holes occur when data packets exceed the default/modified MTU for a network when sending data packets through networks an MTU is established, if the data packet is not fragmented it will not be passed through to its destination.
- When a router processes a data packet that exceeds the MTU for a network it will send an ICMP “destination unreachable” message back to the sending host or is blocked by a fir wall on the sender’s network, the data packet may be dropped.
- Bad modules that convert fiber optic signal into electrical signal can also cause data loss. (i.e. Gigabit interface converter (GBIC) & small form factor pluggable (SFP) are (ISCO router plugins used to convert signals).
- Wrong subnet mask can cause miscommunication & prevent the discovery of network host.
- Wrong gateway address will prevent data from being sent between networks.
- Duplicate IP address will prevent host from accessing the network.
- When having trouble resolving a host name on a network DNS may be down/configured incorrectly.

Experiment :-21

AIM OF THE EXPERIMENT

Lan Design Principles

When designing switched LAN campus network. when nearly 100% of lost CPU cycles on a device such as switch or users computer are consumed by processing broadcast and multicast packets , the network is crippled and unusable . Because of delay inherent in carrier sense multiple access collision detect (CSMA\CD)technologies, such as Ethernet , any more than a small amount of broadcast traffic impacts the operation of devices attached to a switch . Although VLANs reduce the effect of broadcast radiation in LANs, there is still a scaling issue as to how many lost should reside within a given VLAN.

A router provides for larger network designs. Because a VLAN can be segmented depending on traffic patterns within the VLAN .In a network design where traffic is not logically segmented , however a single router . can be burdened with large amount of traffic where the destination LAN is the same as the origination LAN .

Well behaved VLAN

A well-behaved VLAN is not just a VLAN that behaves itself when company is visiting the parents, but it once meant a VLAN in which 80% or more of traffic is to that VLAN .The 80% rule is violated when a user in one VLAN reads mail from a second VLAN , reads & writes to file servers from a 3rd VLAN & sends print jobs to network printers in a fourth VLAN in which 80% or more traffic is to that VLAN. The 80% rule is violated when a user in one VLAN reads mail from a second VLAN, reads & writes to file servers from a 3rd VLAN & second print jobs to network printers in a fourth VLAN .In current network environments the 80/20 rule has given way to the implementation of server forms, which are collection of application servers in a network centric location. The 80/20 rule carried more weight back in the days of slower network connection than what are available today. When you had 10Mbps available to you for user data .For ex-you tried to keep as much as local traffic off the line as you could .In today's enviroment of 100Mbps and 1Gbps network links, however , there is often enough available ,bandwidth that the 80/20 rule has lost its usefulness in network desing.

Available bandwidth supporting muting function:-

Inter-VLAN traffic must be routed .The network desing needs to account for this traffic and allocate enough bandwidth to move inter –VLAN traffic from the source, through the router,to the destination . The amount of bandwidth used between switches needs to be monitored to ensure there is adequate trunk speed fast Ethernet ,Gigabit Ethernet and 10Gigabit by combining multiple fast Ethernet up to to 800Mbps Gigabit Ethernet up to 8Gbps and 10Gigabit Ethernet up to 80Gbps.

Appropriate placement of administrative boundaries:-

Switching flattens network. The deployment of switches outside of your administrative boundary can impact the network within your administrative boundary. If this is the case, your network traffic will be travelling across other networks, essentially trying to find its way on this own rather than being directed by switches.

Experiment :-22

AIM OF THE EXPERIMENT

To configure the primary WAN.

- To configure the settings for the primary WAN(WAN1),Click the edit(pencil) icon.Then use the WAN-Add/edit page to configure the connection.If you enable IPv4/ IPv6 routing mode,complete both tabbed pages.Click Ok to save your settings.Click save to apply your settings to the security appliences.

For IPv4 routing mode,enter the following information the IPv4 tab:-

- Physical port**-**The physical port associated with the primary WAN .
- WAN Name**-**The name of the primary WAN(WAN1)
- DNS server source:-DNS Servers map internet Domain names to IP addresses.You can get DNS server addresses automatically from your ISP or use ISP-specified addresses.

  Get Dynamically from ISP:-

  Choose this option if you have not been assigned a static DNS IP Address.

  Use these DNS servers,Choose this option if you have not been assigned a static DNS IP Address.Also enter the address in the DNS1 & DNS2 fields.

- MAC Address source-
  Specify the MAC address for the primary WAN.Typically you can use the unique 48-bit local Ethernet address of the security appliance as your MAC address source.

-Use default MAC Address:-Choose this option to use the default MAC Address.

-Use the following MAC address:-If your IP required MAC authentication & another MAC Address has been previously registered with your ISP,Choose this option and enter the MAC Address that your ISP requires for this connection.

-MAC Address:-Enter the MAC Address,for ex-01:23:45:67:89:ab

Zone:-Choose the default WAN Zone or an untrusted zone for the primary WAN.You can click the create zone link to view edit or add the zones on the security appliance.

For IPv4/IPv6 routing mode,enter the following information on the IPv6 tab:-

- IP Address assignment:-Choose static IP If your ISP Assigned a fixed(static or permanent) IP Address or choose SLAAC if you were not assigned a static IP Address.Bydefault,your security appliance is configured to be a DHGCPv6 client of the ISP,with stateless address auto configuration.
- SLAAC:-I f you SLAAC,the security appliance can generate its own address using a combination of locally available information and information advertised by routes.
- Static IP:-Enter the static IP address that was provided by your ISP.
- IPv6 Address:-Enter the static IP Address that was provided by your ISP.
- IPv6 prefix length:-The IPv6 network(subnet) is identified by the initial bits of the address called prefix.
- Default IPv6 Gateway:-Enter the IPv6 address of the gateway for your ISP.This is usually provided by the ISP or your network administrator.
- Primary DNS server:-Enter a valid IP Address of the primary DNS SERVERS.
- Secondary DNS Server(optional):-Optionally enter a valid IP Address of the secondary DNS server.

Experiment :-23

AIM OF THE EXPERIMENT

Configure IPv4 and IPv6 on a wireless access point.

Experiment

Configure IPv4

Configure IPv4 DHCP

Step: 1 Log into the web-based utility and choose LAN>IPv4 setting or LAN>VLAN and IPV4 address depending upon the WAP model you have.

Step:2 In this connection type area, click DHCP radio button to automatically obtain IP address. This setting is choosen by default.

Step:3 Choose your preferred DNS configuration from domain name servers radio button.

Step:4 Click save.

Configuration static IPv4 address

Step-1:-Click the ratio button for static IP.

Step-2:-Enter IP address for the access point in the static IP address field .The IP address should be unique & shouldn't have been assigned to any other devices in the same network.

Step-3:- Enter the subnet mask of the network in the subnet mask field. The default mask is based on either the class of IP address you choose, or how many subnets you use for the network.

Step-4:-Enter the default gateway IP address in the default gateway field. A default is a node on the computer that is used when an IP address doesn't match a router in the routine tables.

Experiment :-24

AIM OF THE EXPERIMENT

Introduction to Network programming.

What is network programming?

Networking programming is the act of using computer code to write programs or processes that can communicate with other programs or praesses across a network. Programming use various programming languages, code libraries & protocols to do the word.

What is network programmability?

Network programmability generally refers to tool & best practices for lepioying , managing &troubleshooting network devices.

Main types of networks to program;

Network programming is a rapidly involving discipline. However, engineers programming networks stillneed traditional skills & other knowledge.that knowledge includes understanding that main types of networks that many of to day"s business use.

1. LAN(Local area network)
2. WAN(Wide area network)
3. MAN(Metropolian area network)
4. WLAN(Wireless LAN)
5. VPN (virtual private network)
6. SAN(Storage area network)

Network programming languages-

Network programming for networking engineering pessons& other It pros typically reqires use of an arsay of programming languages & tool.

- Python
- Java
- Perl
- Bash
- Go
- Tcl

Experiment :-25

AIM OF THE EXPERIMENT

Basic Network Troubleshooting Commands.

Description:-

Any computer connected to a network needs to be able to process communication protocols. This requirement has the benefit of offering query commands that give live feedback on different utilities that operate the network. The commands that launch those enquirers provide very useful information for network trouble shooting.

Network commands used in Network trouble shooting:-

- Ping - Ipconfig /Ifconfig
- Telnet - Netstat
- Trace Route -ARP

Ping:-

Ping exploits a feature in the Internet Control Message Protocol. ICMP was specified to provide status feedback on connections and packet transmissions. Ping was these confirmation messages to measure.

Round Trip Time (RTT) on a path to a target.

Ping on windows:-

Important options to try are -

- ? :- Gives the list of options
- a :- Resolve the IP address given to a hostname
- i<number> Minimum no. of hops to cross when replying TTL.
- l <number> size of data payload.
- n <number> No. of requests to send.
- t :- Continuous request issued until the user specifies to stop.
- w <number> -Time out to wait for a response.

Ping output –

The results of the echo requests are shown with the RTT for each request expressed in milliseconds & a summary of statistics for the batch. The window version shows the RTT of each received response in whole milliseconds.

->Telnet –

Ping works at the Network level. It doesn't recognize the session layer concept of ports. Telnet is able to work with ports, so this is the easiest utility to use for a quick check on specific ports. It is a remote terminal protocol & it is one of the oldest TCP/IP protocols, You don't need to log into a remote computer in order to test whether a port is open with Telnet.

Telnet on window & window server :- Although Telnet is bundled into windows, it isn't instantly available you have to enable it.

1. Search for the control panel in the start bar search field.
2. Click on the control panel icon in the search results screen.
3. Select to show large icon in the control panel window.
4. Click on programs & features.

5. Click on turn windows features on or off.
   A popup window will appear.
6. Scroll down in the list of features & check the Telnet Client Box
7. Click OK & wait for the installer to complete.