Cycle No:1

Experiment No:1

**Study of Computer Networks**

**Aim:**

To study the computer networks.

**Theory:**

Computer Networks are interconnection of a number of autonomous computing devices governed by a set of common rules. Here a group of computer systems and other computing hardware devices are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

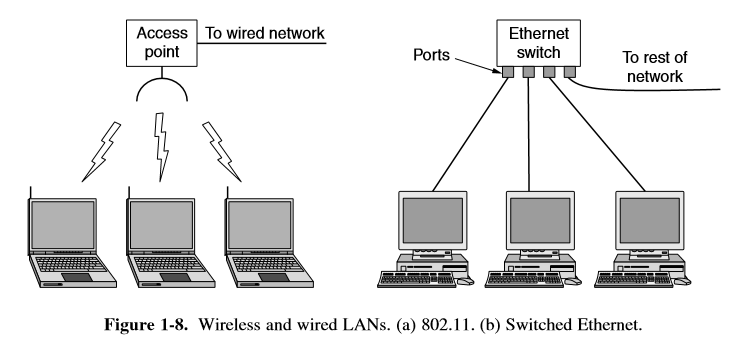
One of the earliest examples of a computer network was a network of communicating computers that functioned as a part of the U.S military’s Semi-Automatic Ground Environment Radar System. In 1969, the University of California at Los Angels, the Stanford Research Institute, the University of California at Santa Barbara and the University of Utah were connected as a part of the ARPANET( It is this network that evolved to become what we now call the internet)

Networks are used to:-

* Facilitate communication via email, video conferencing, instant messaging, etc.
* Enable multiple users to share a single hardware devices like a printer or scanner.
* Enables file sharing across networks.
* Allows for the sharing of software or operating programs on remote systems.
* Make information easier to access and maintain among network users.

Computer networks are often classified in function of the geographical area that they cover:

**LAN(Local Area Network):**

****

A LAN is a network that is used for communicating among computer devices, usually within an office building or home. LAN’s enable the sharing of resources such as files or hardware devices that may be needed by multiple users. Is limited in size, typically spanning a few hundred meters, and no more than a mile. Has lower cost compared to MAN’s or WAN’s. LAN’s can be either wired or wireless. Twisted pair, coax or fibre optic cable can be used in wired LAN’s.

Advantages:

• Speed

• Cost

• Security

• E-mail

• Resource Sharing

Disadvantages:

• Expensive To Install

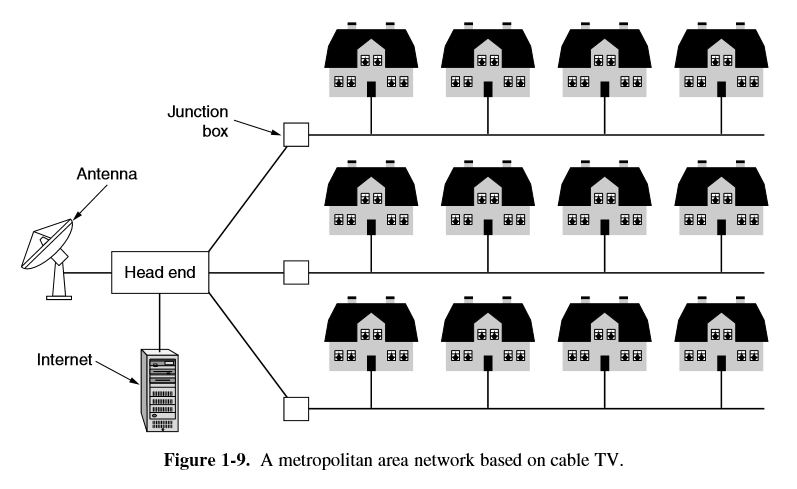
• Requires Administrative Time

• File Server May Fail

• Cables May Break

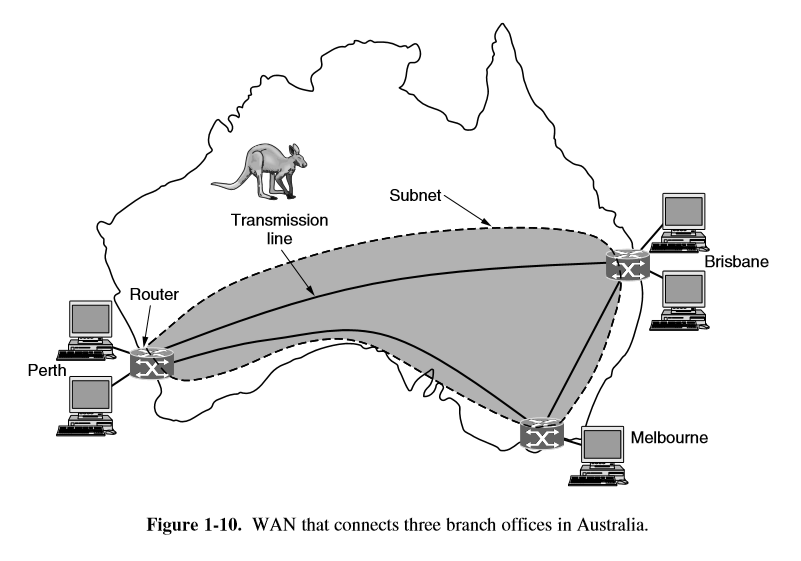
**MAN(Metropolitan Area Network):**

A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus. A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. A MAN often acts as a high speed network to allow sharing of regional resources. A MAN typically covers an area of between 5 and 50 km diameter. Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.



**WAN(WIDE AREA NETWORK):**

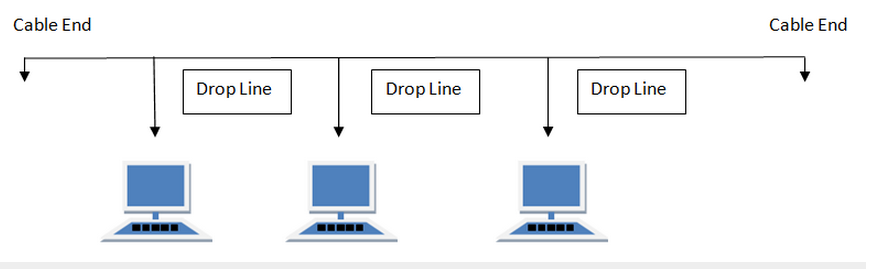
WAN covers a large geographic area such as country, continent or even whole of the world. A WAN is two or more LANs connected together. The LANs can be many miles apart. To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites. Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data. The world's most popular WAN is the Internet.



Another classification of computer networks is based on their physical topology.

**BUS Topology:**

Bus topology is a network type in where every computer and network device is connected to single cable. All hosts are attached to a shared medium, usually a cable through a single interface. Example: early Ethernet networks.



**Features of Bus Topology**

1. It transmits data only in one direction.
2. Every device is connected to a single cable

**Advantages of Bus Topology**

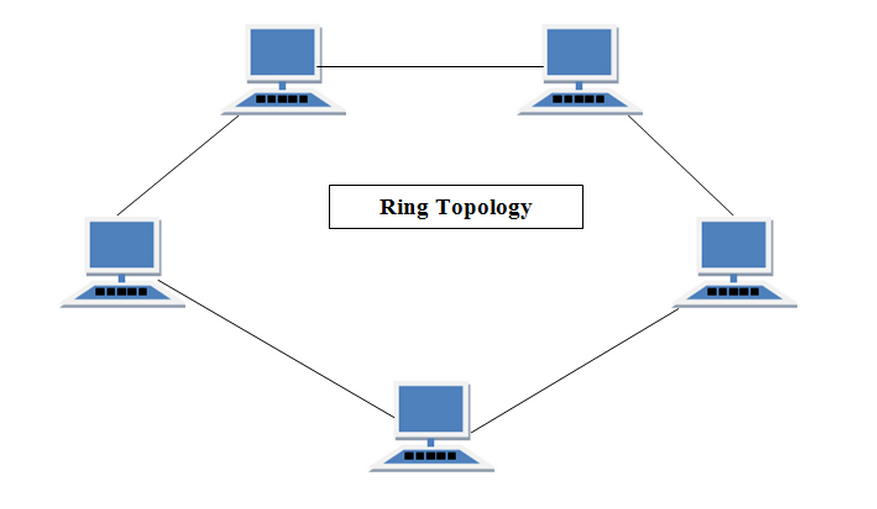
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

**Disadvantages of Bus Topology**

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

**RING Topology**

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device. Each host has a single physical interface connecting to the ring. Any signal sent by the host on the ring will be received by all hosts.



**Features of Ring Topology**

1. A number of repeaters are used and the transmission is unidirectional.
2. Date is transferred in a sequential manner that is bit by bit.

**Advantages of Ring Topology**

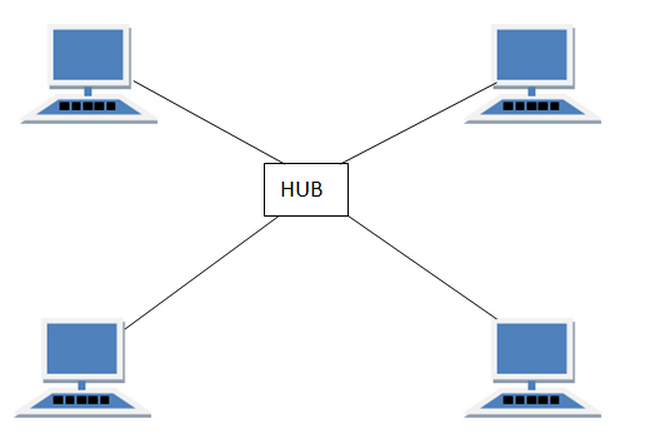
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

**Disadvantages of Ring Topology**

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

**STAR Topology:**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. Hosts have a single physical interface and there is one physical link between each host.



**Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

**Advantages of Star Topology**

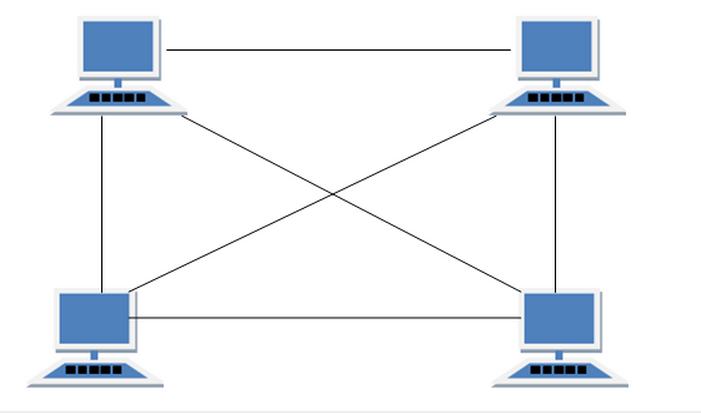
1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed rest of the nodes can work smoothly.

**Disadvantages of Star Topology**

1. Cost of installation is high.
2. Expensive to use.
3. If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity.

**MESH Topology**

It is a point-to-point connection to other nodes or devices. Traffic is carried only between two devices or nodes to which it is connected. To allow any host to sent message to any other host in the network, the easiest resolution is to organize them as a mesh, with a direct and dedicated link between each pan of hosts.



**Features of Mesh Topology**

1. Fully connected.
2. Robust.
3. Not flexible.

**Advantages of Mesh Topology**

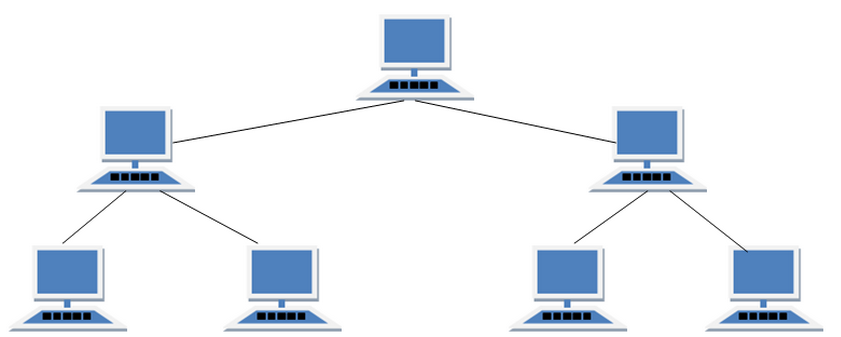
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

**Disadvantages of Mesh Topology**

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

**TREE Topology:**

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy. This is used when a large number of customers must be connected in a very cost effective manner. Example: Cable TV networks.



**Features of Tree Topology**

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

**Advantages of Tree Topology**

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

**Disadvantages of Tree Topology**

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

**COMPONENTS OF COMPUTER NETWORKS:**

The most essential components of a computer network are:

• Network Interface Card

• Hub

• Switch

• Cables and connectors

• Router

• Modem

• Repeater

• Client

• Transmitter

• Bridge

**Network Interface Card:**

Network Interface Card is a device that enables computer to communicate with other computer or network. Using unique hardware address (MAC address) encoded on the card chip, the datalink protocol employs these addresses to discover other systems on the network so that it can transfer data to right destination.

There are two types of NIC - wired and wireless. The wired NIC uses cables and connectors as a medium for data transfer, whereas in wireless card the connection is made using antenna that employs radio wave technology.



**HUB**

A hub is a device that acts as a central connection point for computers on a network. A hub has two different jobs. Its first job is to provide a central point of connection for all of the computers on the network. Every computer plugs into the hub (multiple hubs can be daisy chained together if necessary in order to accommodate more computers).The hub’s other job is to arrange the ports in such a way so that if a PC transmits data, the data is sent over the other computer’s receive wires.

**SWITCH**

A switch performs all of the same basic tasks as a hub. The difference is that when a PC on the network needs to communicate with another PC, the switch uses a set of internal logic circuits to establish a dedicated, logical path between the two PCs. What this means is that the two PCs are free to communicate with each other, without having to worry about collisions. Switches greatly improve a network’s efficiency. Because of the way that switches work, they can establish parallel communications paths.



**CABLES AND CONNECTORS**

Cable is one of the transmission media which can transmit communication signal.

The wired network topology uses special type of cable to connect computers on a network.

There are a number of solid transmission Media types, which are listed below.

**Twisted pair cable** : It is classified as Category 1, 2, 3, 4, 5, 5E, 6 and 7. Category 5E, 6 and 7 are high-speed cables that can transmit 1Gbps or more.

**Coaxial cable :** Coaxial cable more resembles like TV installation cable. It is more expensive than twisted-pair cable but provide high data transmission speed.

**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.

**ROUTERS**

Routers are generally known as intermediate systems, which operates at the network layer of the OSI reference model, routers are devices used to connects two or more networks (IP networks) or a LAN to the Internet.

The router is responsible for the delivery of packets across different networks. The destination of the IP packet might be a web server in another country or an e-mail server on the local area network. It is the responsibility of the router to deliver those packets in a timely manner. The effectiveness of internetwork communications depends on the ability of routers to forward packets in the most efficient way possible.

Routers are now being added to satellites in space. These routers will have the ability to route IP traffic between satellites in space in much the same way that packets are moved on Earth, thereby reducing delays and offering greater networking flexibility.

**MODEM**

A modem enables you to connect your computer to the available internet connection over the existing telephone line. Like NIC, Modem is not integrated with a computer motherboard. It comes as separate part which can be installed on the PCI slots found on motherboard.

A modem is not necessary for LAN, but required for internet connection such as dial-up and DSL.

There are some types of modems, which differs in speed and transmission rate. Standard PC modem or Dial-up modems (56Kb data transmission speed), Cellular modem (used in a laptop that enables to connect while on the go), cable modem (500 times faster than standard modem) and DSL Modems are the most popular.

**REPEATERS**

It is an electronic device that receives a network signal, clears it of unnecessary noise and regenerate it.

**SERVER**

Servers are computers that hold shared files, programs and the network operating system. Server provide access to the network resources to all the users of the network.

**Client**

Servers are computers that access and use the network and shared network resources.

**Transmission Media**

Transmission media are the facilities used to interconnect computers in a network.

**Bridge**

A network bridge connects and filters traffic between two network segments at datalink layer of OSI model.

**Communication Protocol**

It is the set of rules for exchanging information on over the network links. In a protocol stack, each protocol layers the services of protocol below it.

The key elements of a protocol are as follows:

• **Syntax:** Includes such things as data format and signal levels

• **Semantics:** Includes control information for coordination and error handling

• **Timing:** Includes speed matching and sequencing

An important example of protocol stack is HTTP running over TCP over IP over IEEE 802.11. The stack is used between the wireless routers and the PC when some user is surfing the web. Communication protocol may be connection-oriented or connection less, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing.

TCP/IP

It is the foundation of all modern networking. It offers connectionless as well as connection-oriented services over an inherently unreliable network traversed by datagram transmission of IP level.

There is no official TCP/IP protocol model. However, based on the protocol standards that have been developed, we can organize the communication task for TCP/IP into five relatively independent layers, from bottom to top:

• Physical layer

• Network access layer

• Internet layer

• Host-to-host, or transport layer

• Application layer

SUBNETTING AND SUPERNETTING

An IP address is an address used inorder to uniquely identify a device on an IP network. The address is made up of 32 binary bits(IPv4), which can be divisible into a network portion and host portion. The 32 binary bits are broken down into four octets. The value in each octet may range from 0 to 255.

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks – A to E. In Class A address, the first octet is the network portion, and the rest are for the network manager to divide into subnets and hosts. In Class B address, the first two octets are the network portion, rest are for local subnets and hosts. . In Class C address, the first three octets are the network portion, rest are for local subnets and hosts.

Network Mask

A network mask helps to know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C have default masks.

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

SUBNETTING

Subnetting is the process of dividing an IP network into subdivisions called subnets. A subnet is a logical visible subdivision of an IP network. The hosts that belong to a subnet are addressed with a common identical, most-significant bit group in their IP address. This results in the logical division of an IP address into network or routing prefix and host identifier. The routing prefix is expressed in CIDR notation. It is written as the IP address followed by a slash character and some indication of length of mask. The first subnet obtained from subnetting has all bits in the subnet bit group set to 0 and is called subnet 0. The last subnet obtained from subnetting has all bits in the subnet bit group set to 1 and is called all-ones subnet .

Subnetting provides the network administrator with several benefits including extra flexibility, more efficient use of network address and capability to contain broadcast traffic. Variable length subnetting allows an organization to have a mixture of large and small networks and hence better utilization of address space. Subnetting breaks larger networks into smaller networks and the smaller networks are easier to manage. It also allows to apply network security policies at the interconnection between subnets.

If N is the number of bits borrowed from host bits to create subnets, then total number of subnets will be given by 2N and the total number of hosts available per subnet will be 2h, where h is the number of host bits.

Supernetting

Supernetting combines two smaller blocks of contiguous IP address together into a continuous range of address that form a larger supernet. Supernet or supernetwork is an IP network formed from a combination of two or more networks with a common CIDR prefix. The process of forming supernet is called supernetting, prefix aggregation, route aggregation or route summarization.

In internet networking terminology, a supernet is a block of contiguous subnets addressed as a single subnet in a larger network. Supernets always have a subnet mask that is smaller than the masks of the component networks. During the expansion of internet, size of routing tables has also been expanded rapidly.

Supernetting is the process of aggregation routes to multiple smaller networks, thus saving storage space in the routing table and simplifying routing decisions. It also improves the stability of the network by limiting the propagation of routing traffic after a network link fails. It also allows the conservation of address space. The networks would become more efficient because memory is optimized and route information is efficiently shared.

In order for supernetting to work, it needs several routing protocols that actually act in CIDR.

Consider an example ,

Expand the network so that there are twice the number of hosts as before.

192.168.0.0/24

Total number of hosts = 28 = 256

We need 2\*256 = 512 hosts in the new range.

To double the address, we need additional one bit. So

255.255.255.0 11111111.11111111.11111111.00000000

255.255.254.0 11111111.11111111.11111110.00000000 will be the new mask.

Old network address:192d.168d.00000000b.0d

New mask :255d.255d.11111110b.0d

First address will be 192.168.0.0

Last address will be 192.168.1.255

So new network range is from 192.168.0.0 to 192.168.1.255

IPv4

An internet protocol (IP) provides the functionality for interconnecting end systems across multiple networks. For this purpose, IP is implemented in each end system and in routers, which are devices that provide connection between networks.

For decades, the keystone of the TCP/IP protocol architecture has been the Internet Protocol (IP) version 4. The IP header format, which is a minimum of 20 octets, or 160 bits includes the fields:

• Version (4 bits):Indicates version number, to allow evolution of the protocol; the value is 4.

• Internet Header Length (IHL) (4 bits):Length of header in 32-bit words. The minimum value is five, for a minimum header length of 20 octets.

• DS/ECN (8 bits):Prior to the introduction of differentiated services, this field was referred to as the Type of Servicefield and specified reliability, precedence, delay, and throughput parameters. This interpretation has now been superseded. The first 6 bits of the TOS field are now referred to as the DS (Differentiated Services) field. The remaining 2 bits arereserved for an ECN (Explicit Congestion Notification) field.

• Total Length (16 bits):Total IP packet length, in octets.

• Identification (16 bits):A sequence number that, together with the source address, destination address, and user protocol, is intended to identify a packet uniquely.

• Flags (3 bits):Only two of the bits are currently defined. When a packet is fragmented, the More bit indicates whether this is the last fragment in the original packet. The Don't Fragment bit prohibits fragmentation when set. This bit may be useful if it is known that the destination does not have the capability to reassemble fragments. However, if this bit is set, the packet will be discarded if it exceeds the maximum size of an en route subnetwork.Therefore, if the bit is set, it may be advisable to use source routing to avoid subnetworks with small maximum packet size.

• Fragment Offset (13 bits):Indicates where in the original packet this fragment belongs, measured in 64-bit units.

• Time to Live (8 bits):Specifies how long, in seconds, a packet is allowed to remain in the internet. Every router that processes a packet must decrease the TTL by at least one, so the TTL is somewhat similar to a hop count.

• Protocol (8 bits):Indicates the next higher level protocol, which is to receive the data field at the destination; thus, this field identifies the type of the next header in the packet after the IP header.

• Header Checksum (16 bits):An error-detecting code applied to the header only.

• Source Address (32 bits):Coded to allow a variable allocation of bits to specify the network and the end system attached to the specified network (7 and 24 bits, 14 and 16 bits, or 21 and 8 bits).

• Destination Address (32 bits):Same characteristics as source address.

• Options (variable):Encodes the options requested by the sending user; these may include security label, source routing, record routing, and timestamping.

• Padding (variable):Used to ensure that the packet header is a multiple of 32 bits in length.

Cycle No.:1

Experiment No.:1(b)

Date:

**FAMILIARISE COMPUTER NETWORK COMPONENTS**

**AIM**

To familiarize computer network components.

**THEORY**

Cables

Cables are used to connect computers. Although we may use wireless networking, we use cables as well. The most commonly used cables are referred to as category 5 cable RJ-45.

Different types of cables are:

1. Twisted pair cable
2. Coaxial cable
3. Fibre optic cable

Twisted pair Cable :

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. . One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



Unshielded twisted pair standards:

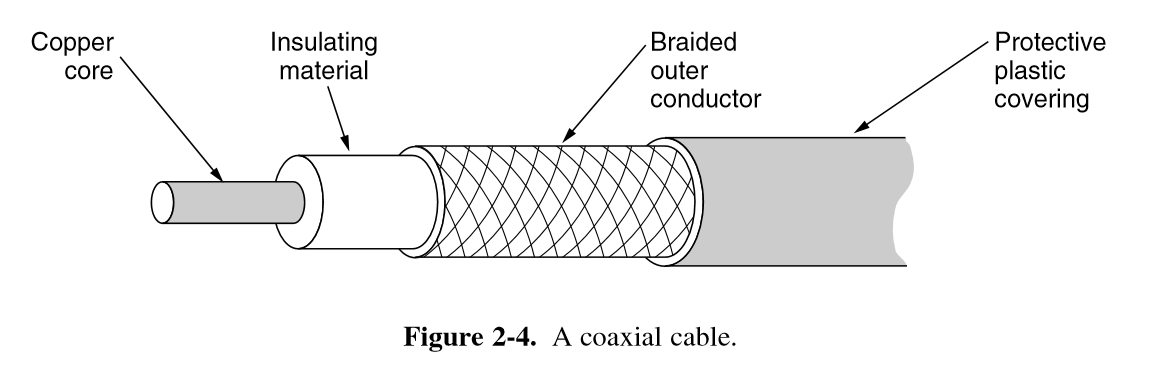
Two UTP cable termination standards are EIA/TIA 568A and EIA/TIA 568B. EIA/TIA 568A is a set of telecommunication standards from TIA. The intent of these standards is to provide recommended practices for the design and installation of cabling systems. EIA/TIA 568A recommends the are T 568A pinout for horizontal cables. It also allows are T 568B as an alternative to accommodate 8-pin cabling systems.



Coaxial Cable

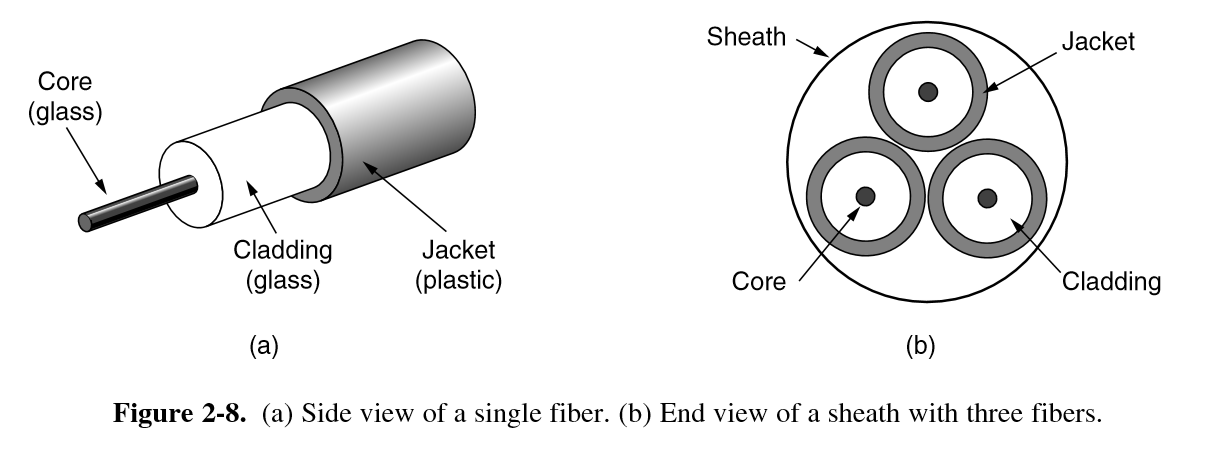
Coaxial cable has two wires of copper. The core wire lies in center and is made of solid conductor. Core is enclosed in an insulating sheath. Over the sheath the second wire is wrapped around and that too in turn encased by insulator sheath. This all is covered by plastic cover. Because of its structure coax cables are capable of carrying high frequency signals than that of twisted pair cables. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of Coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet) and RG-11 (Thick Ethernet. RG stands for Radio Government. Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.



  
Fiber-optic cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Propagation Modes

Multimode:

Multimode is so named because multiple beams from a light source

move through the core in different paths.

In multimode step-index fiber, the density of the core remains constant from the

center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A second type of fiber, called multimode graded-index fiber, decreases this distortion

of the signal through the cable. The word *index* here refers to the index of refraction.

As we saw above, the index of refraction is related to density. A graded-index fiber,

therefore, is one with varying densities.

Cycle No.:1

Experiment No.:2

Date:

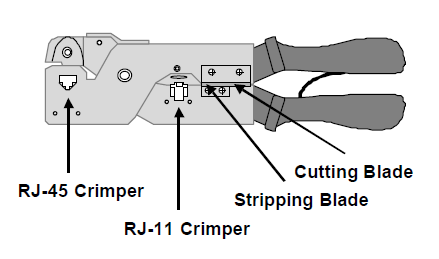
**CRIMPING OF UTP CABLES**

**AIM**

To crimp UTP cables to make direct cables.

**MATERIALS REQUIRED**

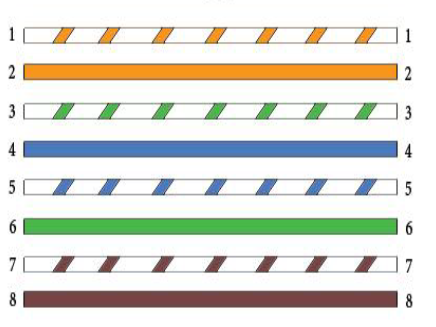
UTP cable, Crimping tool, two RJ-45 connectors



CRIMPING TOOL

**PROCEDURE:**

1. Strip off about 13mm of the plastic jacket off the end of the UTP cable. The ends must be cut squarely, not diagonally. To cut the cable, insert it between the cutting blades and squeeze the crimper handles firmly .Care must be taken not to cut into the wires.
2. Spread the wires apart and flatten them out.
3. Sort the wires in the following order from left to right – white/orange, orange, white/green, blue, white/blue, green, white/brown and brown.
4. Make sure that all wires are of same length. If necessary use crimping tool or wire stripper to trim the wires.
5. Insert the eight wires into RJ-45 connector and push them until all the wires reach the end of the connector. The ends of the wires must make direct contact with metal pins at the tip of the connector.
6. Insert the connector into RJ-45 crimping slot and crimp them.
7. Repeat the steps from 1 to 6 for the other end of the cable.
8. Ensure that none of the wires appears outside RJ-45 connector on both ends of the cable.
9. Test the completed direct cable by connecting it to the system and the other end to the RJ-45 female connector.
10. Use the command ifconfig to get the IP address and use the command ‘ping ip\_address’ command to verify that the connection is complete. If the connection is not successful error message will be displayed.



**RESULT**

The experiment to crimp UTP cables to make direct cables has been completed successfully.

Cycle No.:1

Experiment No.:3

Date:

**SUBNETTING AND SUPERNETTING**

**AIM**

Write a program in Python to find number of networks, number of subnetworks, number of hosts in each subnet, and all hosts in each subnet for a given network.

**ALGORITHM**

1. Start
2. Initialize the variables no\_of\_networks, no\_of\_hosts, count=0 and octet=0, q, r, len, a, pow, snt=0;
3. Enter the IP address as a string.
4. Calculate the length of the string using strlen function into a variable ‘len’
5. Copy each characters of the string to the variable ‘c’.
6. Check whether the characters are ‘.’,’/’ or eof.

If not equal, copy the values to ‘a’.

* 1. Find the octet value using the equation. Octet=octet\*10+b;
  2. Else assign byte[count]=octet; Increment the count; Assign octet=0;

1. Subnet=byte[4];

q=subnet/8;

r=subnet%8;

pow=8\*q;

1. Calculate no\_of\_network=(int)pow(2,power), no\_of\_subnet=(int)power(2,r)-2, no\_of\_host=(int)pow(2,32-no\_of\_subnet)-2;
2. Printing the subnets

Increment=(int)pow(2,8-r);

byte[q]=incr;

* 1. While(q<4)

{

byte[++q]=0;

}

* 1. While(snt<=no\_of\_subnet)

{

Printf(“%d.%d.%d.%d”,byte[0],byte[1],byte[2],byte[3];)

byte[q]+=incr;

snt++;

}

Cycle No.:1

Experiment No.:4

Date:

**VLAN**

**AIM**

Create VLAN using switches and routers.

**THEORY**

VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a modern way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones.

By using VLAN a network administrator will be able to group together stations by logical function, or by applications, without regard to physical location of the users.Each VLAN functions as a separate LAN and spans one or more switches. This allows host devices to behave as if they were on the same network segment.

VLAN has three major functions:

* Limits the size of broadcast domains
* Improves network performance
* Provides a level of security

VLANs group stations belonging to one or more physical LANs into broadcast domain. The stations in a VLAN communicate with one another as though they belong to same physical segment.

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

VLAN Modes

VLAN switching mode: The VLAN forms a switching bridge in which frames are forwarded unmodified.

VLAN translation mode : It is used when frame tagging method is changed in the network path.

VLAN routing mode : When a packet is routed from VLAN to another, we use VLAN routing mode.

PROCEDURE

1. Select three machines.
2. Assign IP address to each of the systems such that they belong to the same network, using the command

*sudo ifconfig eth0 ip\_address*

1. Verify if the IP has been set using the command ‘*ifconfig*’.
2. Open the browser to get the web interface of the Layer 2 switch at 192.168.100.128
3. Login with required credentials.
4. Select VLAN in all options under the Network tab.
5. Edit the default or existing VLAN to free up ports for creating new VLAN.
6. Assign a new VLAN id and allot the ports for the new VLAN created.
7. Create one more VLAN in the similar way and assign the free ports.
8. Connect PC1 to a port in VLAN1 and PC2 and PC3 to ports allotted in VLAN2.
9. Ping from PC1 to PC2 to check that no communication occurs between PCs in VLAN1 and VLAN2 though they are in the same network.

Command:*ping ip\_address \_of\_ PC1*

It shows host unreachable.

1. Ping from PC2 to PC3 to check whether communication occurs between them.

Command:*ping ip\_address \_of\_ PC3*

It shows reply from PC3.

RESULT

Two VLANs are set up using switches and routers and its working has been observed.