Cycle No:1

Expt No:1

Date:16/7/2015

**STUDY OF COMPUTER NETWORKS**

**AIM**

Study of computer networks, components, types of networks, subnetting and supernetting.

**THEORY**

Computer networks is the inter connection of autonomous computing devices which are governed by a set of rules, that is a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via copper wire, fibre optics, microwaves, infrared and communication satellites can also be used. Networks come in many sizes, shapes and forms and they are usually connected together to make larger networks, with the internet being the most well known example of a network of networks. The difference between a computer network and a distrtibuted system is that in a distributed system, a collection of independent computers appears to its users as a single coherent system.

**BASIC COMPUTER NETWORK COMPONENTS**

**Network Interface Card**

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

**Hub**

Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not. Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switches and Routers.**

**Switch**

Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses **physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port.

Like Hub, switch don’t broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

**Cables and connectors**

Cable is one way of transmission media which can transmit communication signals. The wired network typology uses special type of cable to connect computers on a network.

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

**Twisted pair wire**

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.

**Router**

The device that is used to **connect a LAN with an internet connection is called Router**. When you have **two distinct networks** (LANs) or want to share a single internet connection to multiple computers, we use a Router.

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

**Communication Protocol**

When computers, terminals, and/or other data processing devices exchange data, the procedures involved can be quite complex. Consider, for example, the transfer of a file between two computers. There must be a data path between the two computers, either directly or via a communication network.

A protocolis used for communication between entities in different systems. The protocol, can be defined as a set of rules governing the exchange of data between two entities.

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

**TCP**

In general terms, communications can be said to involve three agents: applications, computers, and networks. Examples of applications include file transfer and electronic mail. The applications that we are concerned with here are distributed applications that involve the exchange of data between two computer systems. These applications, and others, execute on computers that can often support multiple simultaneous applications. Computers are connected to networks, and the data to be exchanged are transferred by the network from one computer to another. Thus, the transfer of data from one application to another involves first getting the data to the computer in which the application resides and then getting the data to the intended application within the computer. 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

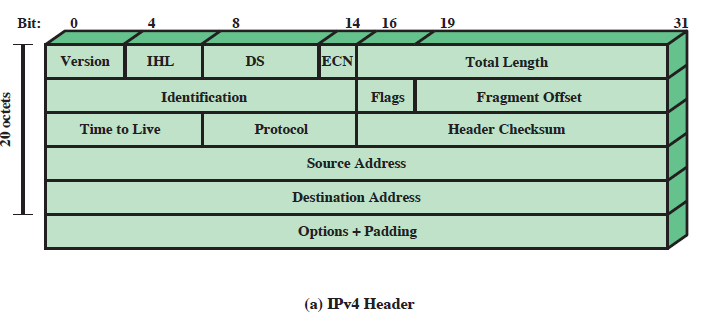
• Application layer

**IP**

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. Higher-level data at a source end system are encapsulated in an IP protocol data unit (PDU) for transmission. This PDU is then passed through one or more networks and connecting routers to reach the destination end system

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



The fields are:

• **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 Service** field and specified reliability, precedence, delay, and throughput parameters.

• **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.

• **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.

.

• **Protocol (8 bits):** Indicates the next higher level protocol, which is to receive the data field at the destination.

• **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.

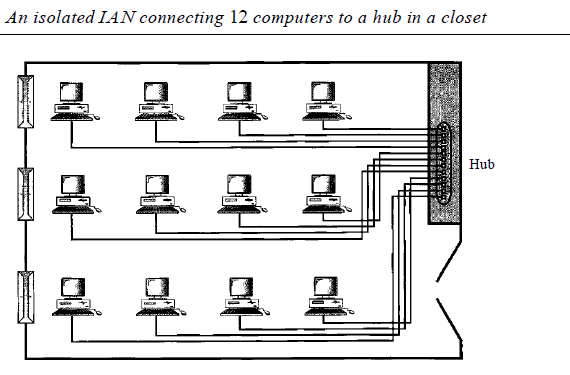
**TYPES OF NETWORKS**

The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 m; aWAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

**Local Area Network**

A local area network (LAN) is usually privately owned and links the devices in a single

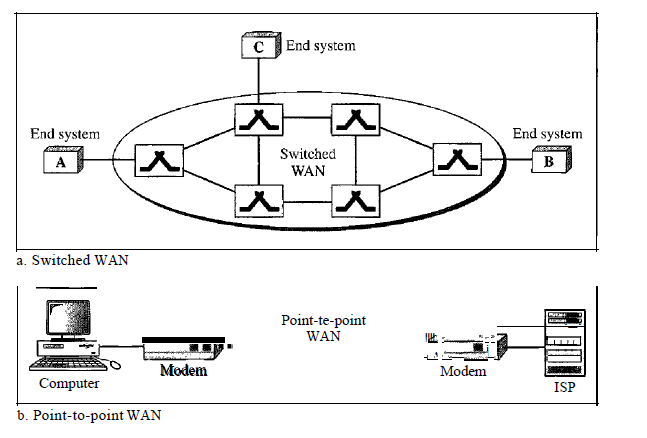
office, building, or campus . Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.



**WIDE AREA NETWORK**

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider This type of WAN

is often used to provide Internet access.

****

**Metropolitan Area Networks**

A metropolitan area network (MAN) is a network with a size between a LAN and a

WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.

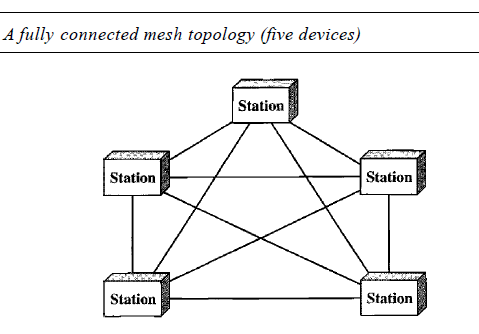
**NETWORK TOPOLOGY**

The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

**Mesh**

In a mesh topology, every device has a dedicated point-to-point link to every

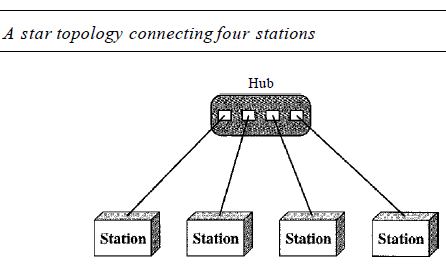
other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.



**Star**

In a star topology, each device has a dedicated point-to-point link

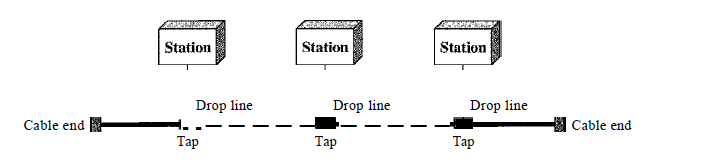
only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .



**Bus**

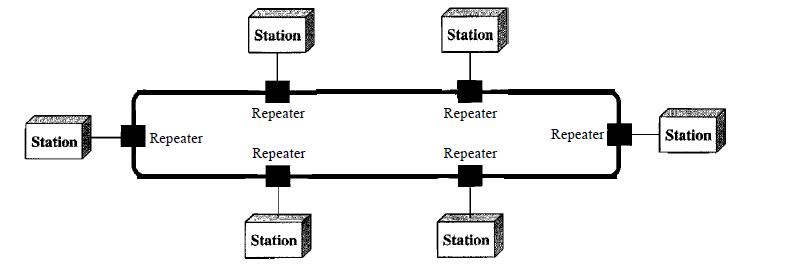
A bus topology**,** on the other hand, is multipoint. One long cable acts as a backboneto link allthe devices in a network Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact withthe metallic core. As a signal travels along the backbone, some of its energy is transformedinto heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For

this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



**Ring**

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



**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, which can be divisible into a network portion and host portion. The 32 binary bits are broken down into four octets. Each octet is converted into decimal seperated by a period. The value in each octet may range from 0 to 255(decimal)

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. Octet 2, 3and 4 are for network manager to divide into subnets and hosts. In class B address, the first two octets are the network portion. Octet 3and 4 are for local subnets. In class C address, the first three octets are the network portion. Octet 4 is for local subnets and hosts.

**Network Mask**

A Network Mask helps to know which portion of the address identify the network and which portion of address identifies the node.

Class A, B and C have default mask.

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 host that belongs 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 hosts identifier. The routing prefix is expressed in CIDR notation.

It is written as the IP address followed by a slash character and some indications of length of the mask(for eg:-176.16.0.0/16). The first subnet obtained from subnetting has all bits in the subnet bit group set to 0 and it is called subnet 0. The last subnet obtained from subnetting has all bits in the subnet group set to 1 and it is called all 1 subnet.

Subnetting provides the network administrator with several benefits including extra flexibility, more efficient use of network address and the 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 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 bit to create subnets, then total number of subnets will be given by 2^N and total number of hosts available per subnet will be 2 ^h, h is the number of host bit.

**SUPERNETTING**

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

In internet networking terminology, a super net is a block of contiguous subnetworks addressed as a single subnet work in larger networks. Supernet always has a subnet mask that is smaller than the mask of component network. 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 division. It also improves the stability of the network by limiting the propogation of routing traffic after a network link phase. It also allows conservation of address space. The network would become more efficient because memory storage is optimized and route information is efficiently shared.

**RESULT**

Study of computer networks, components, types of networks, subnetting and supernetting has been completed successfully.

Cycle No:1

Expt No:2

Date:16/7/2015

**NETWORK COMPONENTS**

**AIM**

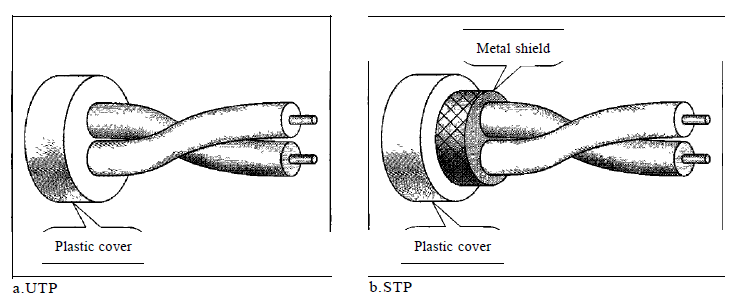
To familiarize with computer network components like cables, connectors, hubs, switches, routers and network cards

THEORY

**CABLES AND CONNECTORS**

A transmission medium that is anything that can carry information from a source to a destination

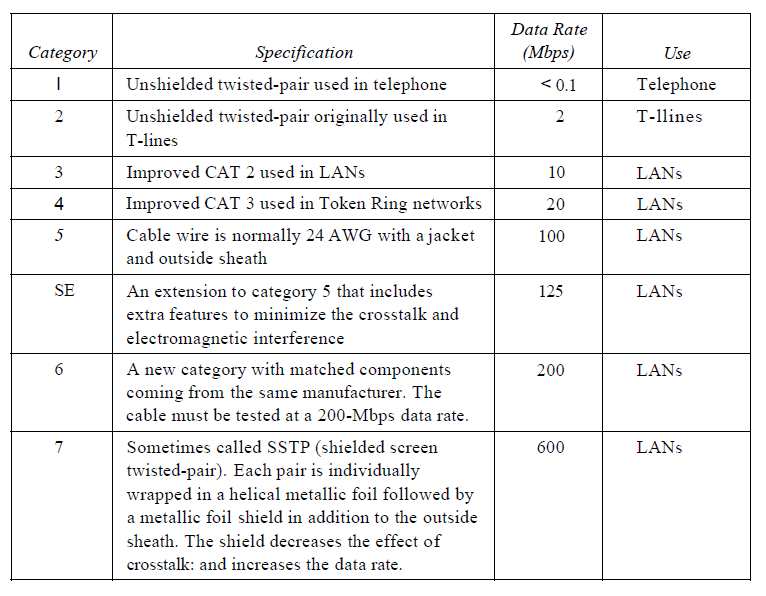
A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.



**Unshielded Versus Shielded Twisted-Pair Cable**

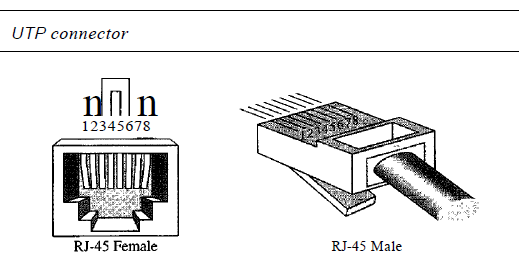
The most common twisted-pair cable used in communications is referred to as

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. Figure below shows categories of UTP



**Connectors**

The most common UTP connector is RJ45 (RJ stands for registered jack). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.



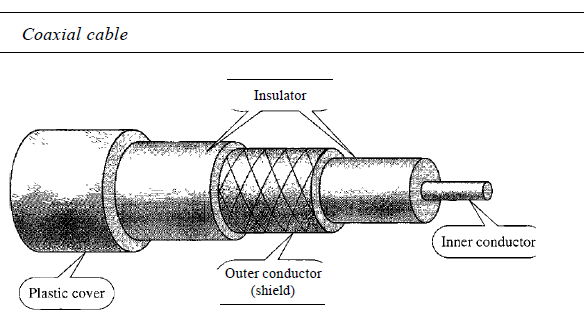
**Coaxial Cable**

Coaxial cable carries signals of higher frequency ranges than those in twisted pair

cable, in part because the two media are constructed quite differently. Instead of

having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is

protected by a plastic cover.



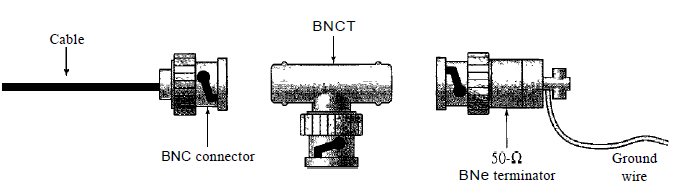
**Coaxial Cable Standards**

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

**Coaxial Cable Connectors**

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch

out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.



**Fiber-Optic Cable**

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

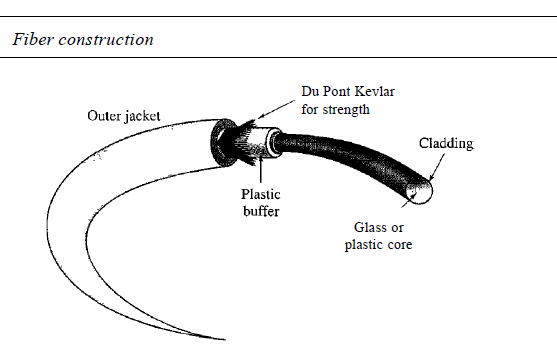
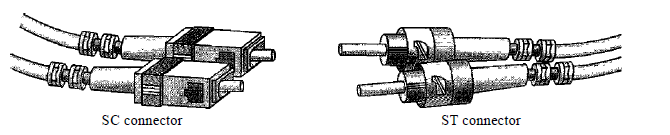


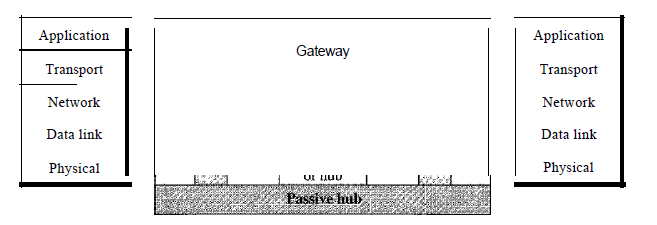
Figure below shows the fibre optic cable connectors



**HUB**:-A hub has a number of input lines that it joins electrically. Frames arriving on any of the lines are sent out on all the others. If two frames arrive at the same time, they will collide, just as on a coaxial cable. In other words, the entire hub forms a single collision domain. All the lines coming into a hub must operate at the same speed. Hubs differ from repeaters in that they do not (usually) amplify the incoming signals and are designed to hold multiple line cards each with multiple inputs, but the differences are slight. Like repeaters, hubs do not examine the 802 addresses or use them in any way. Now let us move up to the data link layer where we find bridges and switches.,A bridge connects two or more LANs. When a frame arrives, software in the bridge extracts the destination address from the frame header and looks it up in a table to see where to send the frame. With a bridge, each line is its own collision domain, in contrast to a hub.

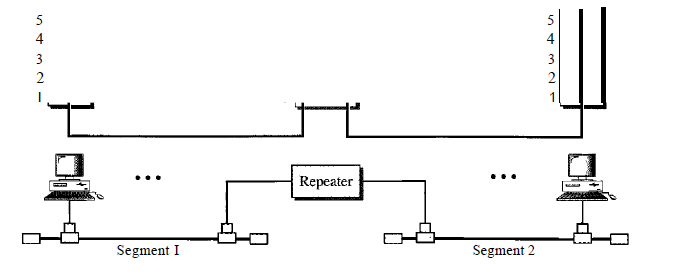
**Passive Hubs**

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.



**Active Hubs**

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. Hubs can also be used to create multiple levels of hierarchy. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).



**SWITCHES**

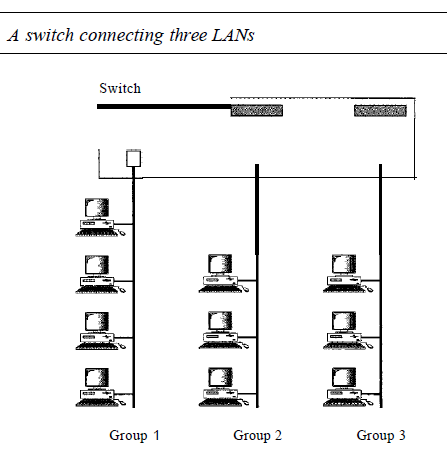
Switches are similar to bridges in that both route on frame addresses. In fact, many people uses the terms interchangeably. Since each switch port usually goes to a single computer, switches must have space for many more line cards than do bridges intended to connect only LANs. Each line card provides buffer space for frames arriving on its ports. Since each port is its own collision domain, switches never lose frames to collisions. However, if frames come in faster than they can be retransmitted, the switch may run out of buffer space and have to start discarding frames.

**Two-Layer Switches**

We can have a two-layer switch or a three-layer switch. A **three-layer switch** is used at the network layer; it is a kind of router. The **two-layer switch** performs at the physical and data link layers. A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision, as we saw in Ethernet).

A two-layer switch, as a bridge does, makes a filtering decision based on the MAC

address of the frame it received. However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing. It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

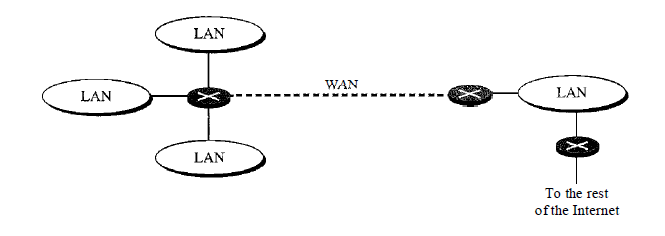


**Three-Layer Switches**

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding. In this book, we use the terms routerand three-layer *switch* interchangeably.

**Router**

When a packet comes into a router, the frame header and trailer are stripped off and the packet located in the frame's payload field is passed to the routing software. This software uses the packet header to choose an output line. For an IP packet, the packet header will contain a 32-bit (IPv4) or 128-bit (IPv6) address, but not a 48-bit 802 address. The routing software does not see the frame addresses and does not even know whether the packet came in on a LAN or a point-to-point line. Figure shows routers connecting LAN s and WAN s.



.

**Bridges**

A bridge operates in both the physical and the data link layer. As a physical layer

device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame. A bridge has a table nsed in filtering decisions. A bridge does not change the physical (MAC) addresses in a frame. A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary. According to the IEEE 802.1 d specification, a system equipped with transparent bridges must meet three criteria:

I. Frames must be forwarded from one station to another.

2. The forwarding table is automatically made by learning frame movements in the

network.

3. Loops in the system must be prevented.

**Network Interface Card**

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

There are **two types of network cards: wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

**RESULT**

Familiarization of computer network components like cables, connectors, hubs, switches, routers and network cards has been completed successfully.

]

Cycle No:1

Expt No:3

Date:23/7/2015

CRIMPING

**AIM**

To crimp UTP cables to make direct cables.

**PROCEDURE**

**Step 1-**Unroll the required length of network cable

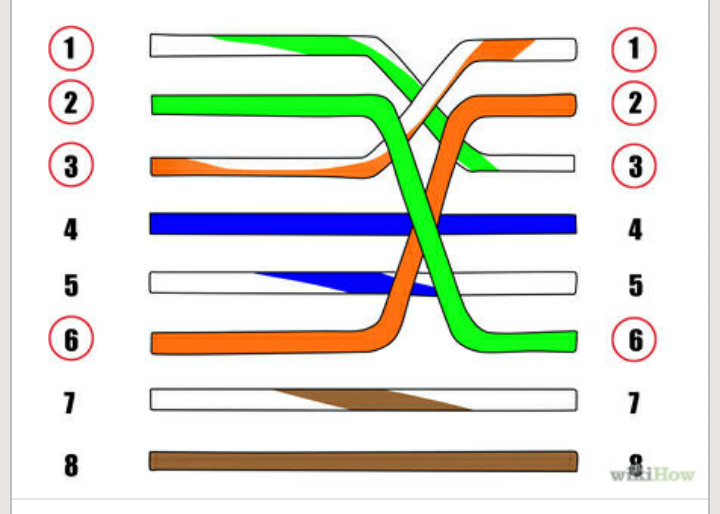
**Step 2-**Carefully remove the outer jacket of the cable. Be careful when stripping the jacket as to not cut the internal wiring.

**Step 3-**Inspect the newly revealed wires for any cuts that expose the copper wire inside**.** If we have removed the protective sheath of any wire, we will need to cut the entire segment of wires off and start over at step one.

**Step 4-**Untwist the pairs so they will lay flat between our fingers. The white piece of thread can be cut off.

**Step 5-**Arrange the wires based on the wiring specifications we are following**.** There are two methods set by the TIA, 568A and 568B. Which one you use will depend on what is being connected. A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC).Two like devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568B, while a cross-over cable has one end wired 568A and the other end wired 568B. Here we are using 568B.So put the wires in the following order, from left to right:

* + white orange
  + orange
  + white green
  + blue
  + white blue
  + green
  + white brown
  + brown



* 568A - from left to right:
  + white/green
  + green
  + white/orange
  + blue
  + white/blue
  + orange
  + white/brown
  + brown

**Step 6-**Press all the wires flat and parallel between your thumb and forefinger**.** Verify the colors have remained in the correct order. Cut the top of the wires.

**Step 7-**Keep the wires flat and in order as we push them into the RJ-45 connector with the flat surface of the plug on top. The white/orange wire should be on the left if we're looking down at the jack.

**Step 8-**Place the wired plug into the crimping tool. Give the handle a firm squeeze. We should hear a ratcheting noise as we continue. Once we have completed the crimp, the handle will reset to the open position..

**Step 9-**Repeat all of the above steps with the other end of the cable.

**Step 10-** Test the cable to ensure that it will function in the field.

**RESULT**

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

Cycle No:1

Expt No:4

Date:13/8/2015

**SUBNETTING**

**AIM**

Write a program in python to find number of networks, number of hosts, different subnets and all the host addresses in each subnet for a given network.

**THEORY**

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, which can be divisible into a network portion and host portion. The 32 binary bits are broken down into four octets. Each octet is converted into decimal seperated by a period. The value in each octet may range from 0 to 255(decimal)

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. Octet 2, 3and 4 are for network manager to divide into subnets and hosts. In class B address, the first two octets are the network portion. Octet 3and 4 are for local subnets. In class C address, the first three octets are the network portion. Octet 4 is for local subnets and hosts.

**Network Mask**

A Network Mask helps to know which portion of the address identify the network and which portion of address identifies the node.

Class A, B and C have default mask.

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 host that belongs 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 hosts identifier. The routing prefix is expressed in CIDR notation.

It is written as the IP address followed by a slash character and some indications of length of the mask(for eg:-176.16.0.0/16). The first subnet obtained from subnetting has all bits in the subnet bit group set to 0 and it is called subnet 0. The last subnet obtained from subnetting has all bits in the subnet group set to 1 and it is called all 1 subnet.

Subnetting provides the network administrator with several benefits including extra flexibility, more efficient use of network address and the 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 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 bit to create subnets, then total number of subnets will be given by 2^N and total number of hosts available per subnet will be 2 ^h, h is the number of host bit.

**ALGORITHM**

**Step 1-**Start

**Step 2-**Initialise the variables str[15], leng, c, digit, sum=0, arr[5], count=0, subnet, qu, rem, incr, snt=0

**Step 3-**Read the IP address as a string str

**Step 4-**Store the string length into variable leng

**Step 5-**for(i=0 to leng)

**Step 5.1-**copy each character of string str to a variable c

**Step 5.2-**check whether c!=’.’ or ‘\0’ or ‘/’

**Step 5.2.1-**if yes

copy the integer value of c into digit

calculate sum=sum\*10+digit

**Step 5.2.2-**else

copy sum into arr[count]

increment count

assign sum=0

**Step 6-**assign subnet=arr[4]

**Step 7-**calculate qu=subnet/8

**Step 8-**calculate rem=subnet%8

**Step 9-**calculate power=8\*qu

**Step 10-**to calculate

no\_ntw=2^power

no\_subnet=2^rem-2

no\_host=2^(32-subnet)-2

**Step 11-**To print subnets,calculate incr=2^(8-rem)

**Step 12-**Assign array[qu]=incr

**Step 13-**Till qu less than 4

Arr[++qu]=0

**Step 14-**To print subnet

**Step 14.1-**While(snt<=no\_subnet)

**Step 14.1.1-**Display arr[0], arr[1], arr[2]

**Step 14.1.2-** Increment qu as qu+=incr

**Step 14.1.3-**Increment snt

Cycle No:1

Expt No:5

Date:18/8/2015

**VLAN**

**AIM**

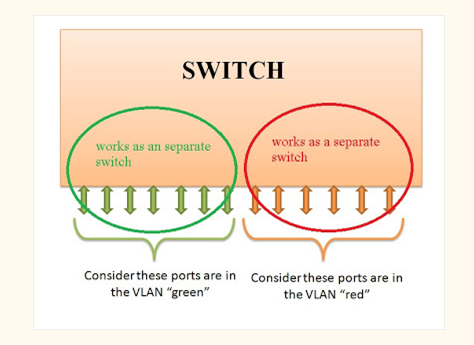
To create VLAN using switches and routers.

**THEORY**

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic. We can define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring. The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments. A LAN can be divided into several logical LANs called VLANs. Each VLAN is a work group in the organization. If a person moves from one group to another, there is no need to change the physical configuration. The group membership in VLANs is defined by software, not hardware. Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN. This means if a station moves from VLAN 1 to VLAN 2, it receives broadcast messages

sent to VLAN 2, but no longer receives broadcast messages sent to VLAN 1. VLAN technology even allows the grouping of stations connected to different

switches in a VLAN.



**VIRTUAL TRUNK PROTOCOL (VTP)**

VTP, a Cisco proprietary protocol, was designed by Cisco with the network engineer and administrator in mind, reducing the administration overhead and the possibility of error in any switched network environment. When a new VLAN is created and configured on a switch without the VTP protocol enabled, this must be manually replicated to all switches on the network so they are all aware of the newly created VLAN. This means that the administrator must configure each switch separately, a task that requires a lot of time and adds a considerable amount of overhead depending on the size of the network. The configuration of a VLAN includes the VLAN number, name and a few more parameters. This information is then stored on each switch's NVRAM and any VLAN changes made to any switch must again be replicated manually on all switches.

**VTP MODES**

The VTP protocol is a fairly complex protocol, but easy to understand and implement once we get to know it. Currently, 3 different versions of the protocol exist, that is, version 1, 2 and 3, with the first version being used in most networks. Despite the variety of versions, it also operates in 3 different modes: Server, client and transparent mode, giving us maximum flexibility on how changes in the network effect the rest of our switches.

* VTP Server mode
* VTP Client mode
* VTP Transparent mode

Each mode has been designed to cover specific network setups and needs, A typical setup involves at least one switch configured as a VTP Server, and multiple switches configured as VTP Clients. The logic behind this setup is that all information regarding VLANs is stored only on the VTP Server switch from which all clients are updated. Any change in the VLAN database will trigger an update from the VTP Server towards all VTP clients so they can update their database. Lastly, be informed that these VTP updates will only traverse Trunk links. This means that you must ensure that all switches connect to the network backbone via Trunk links, otherwise no VTP updates will get to your switches.

#### VTP SERVER MODE

By default all switches are configured as VTP Servers when first powered on. All VLAN information such as VLAN number and VLAN name is stored locally, on a separate NVRAM from where the 'startup-config' is stored. This happens only when the switch is in VTP Server mode.

For small networks with a limited number of switches and VLANs, storing all VLAN information on every switch is usually not a problem, but as the network expands and VLANs increase in number, it becomes a problem and a decision must be made to select a few powerful switches as the VTP Servers while configuring all other switches to VTP Client mode.

#### VTP CLIENT MODE

In Client Mode, a switch will accept and store in its RAM all VLAN information received from the VTP Server, however, this information is also saved in NVRAM, so if the switch is powered off, it won't loose its VLAN information.

The VTP Client behaves like a VTP Server, but we are unable to create, modify or delete VLAN's on it.

If, for any reason, two clients are cascaded together, then the information will propagate downwards via the available Trunk links, ensuring it reaches all switches:

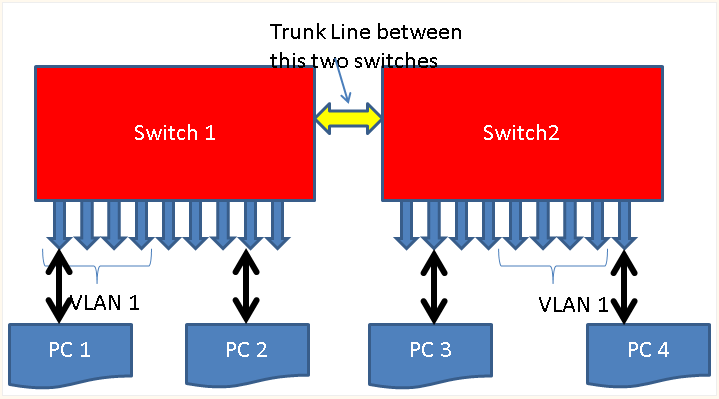
#### VTP TRANSPARENT MODE

The VTP Transparent mode is something between a VTP Server and a VTP Client but does not participate in the VTP Domain.

In Transparent mode, we are able to create, modify and delete VLANs on the local switch, without affecting any other switches regardless of the mode they might be in. Most importantly, if the transparently configured switch receives an advertisement containing VLAN information, it will ignore it but at the same time forward it out its trunk ports to any other switches it might be connected to.

Lastly, all switches configured to operate in Transparent mode save their configuration in their NVRAM (just like all the previous two modes) but not to advertise any VLAN information of its own, even though it will happily forward any VTP information received from the rest of the network.

This important functionality allows transparently configured switches to be placed anywhere within the network, without any implications to the rest of the network because as mentioned, they act as a repeater for any VLAN information received:



**PROCEDURE**

**Step 1**-Connect sysytems to switch using UTP cables. System 1 to port 3, System 2 to port 11, System 3 to port 18.

**Step 2**-Assign IP address to systems as 192.168.100.123, 192.168.100.125, 192.168.100.127 using command ifconfig eth0 ip\_address

**Step 3**-Give default IP address of the switch that is 192.168.100.128 in the browser.

**Step 4**-Select VLAN from the options given.

**Step 5**-Delete the default VLAN

**Step 6**-Group by entering the VLAN description and port details as:

VLAN1 and ports are 2,3,4

VLAN2 and ports are 9, 10, 11, 12

VLAN3 and ports are 17, 18, 19, 20

**Step 7**-Repeat step no 6 if more number of VLANS are required.

**Step 8**-Check whether the sysytems in different VLAN can communicate using the ping command that is in the computer in which IP address is 192.168.100.125

**Step 9**-Since this system belongs to another VLAN (as port 11 is in VLAN2), communication is not possible.

**Step 10**-Repeat step 8 and 9 for same system with IP address 192.168.100.127

**Step 11**-Since this system also belongs to another VLAN VLAN (as port 18 is in VLAN3), communication is not possible.

**Step 12**-Change the cable from port 11 to port 4,so that two systems are in VLAN1.

**Step 13**-Check whether systems in same VLAN can communicate with each other using ping command, that is ping 192.168.100.125

**Step 13**-The two systems are in VLAN1, therefore communication is possible.

**Step 14**-Stop

**RESULT**

Creating VLAN s using switches and routers experiment has been completed successfully.