**COMPUTER NETWORKS LAB (NCS- 651)**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VIDYA COLLEGE OF ENGINEERING

MEERUT

BATCH 2015-2019

****

**SUBMITTED TO: SUBMITTED BY:**

MR. ASHWINI VASHISHTHA VINEET KUMAR

(CSE&IT DEPT.) **(1522910111)**

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **EXP NO.** | **EXPERIMENT NAME** | **DATE** | **SIGNATURE** |
| **1.** | **STUDY OF INTERNAL PARTS F THE SYSTEM** | **05/02/2018** |  |
| **2.** | **STUDY OF NETWORKING DEVICES IN DETAIL** | **12/02/2018** |  |
| **3.** | **CONNECT COMPUTERS IN LAN** | **19/02/2018** |  |
| **4.** | **CCTV SURVEILLANCE** | **26/02/2018** |  |
| **5.** | **CONFIGURE NETWORK TOPOLOGIES** | **12/03/2018** |  |
| **6.** | **STUDY OF BIT STUFFING IN FRAMES** | **19/03/2018** |  |
| **7.** | **STUDY OF BYTE STUFFING IN FRAMES** | **26/03/2018** |  |
| **8.** | **STUDY OF CHARACTER STUFFING IN FRAMES** | **09/04/2018** |  |
| **9.** | **STUDY OF CYCLIC REDUNDANCY CHECK IN DATA** | **16/03/2018** |  |

EXPERIMENT NO. 1

**AIM : Study of Internal Parts of Computer.**

**RAM(RANDOM ACCESS MEMORY):**

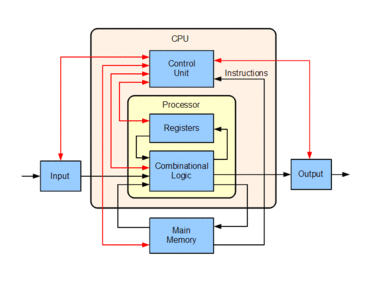
Random-access memory (RAM) is a type of computer data storage. A RAM device makes it possible to access data in random order, which makes it very fast to find a specific piece of information. Certain other types of storage are not random-access. For example, a hard disk drive and a CD will read and write data in a predetermined order. The mechanical design of these devices prescribes that data access is consecutive. This means that the time it takes to find a specific piece of information can vary greatly depending on where it is located on the disk.

RAM devices are used in computer systems as the main memory. RAM is considered volatile memory, which means that the stored information is lost when there is no power. So, RAM is used by the central processing unit (CPU) when a computer is running to store information that it needs to be used very quickly, but it does not store any information permanently.



**CPU (CENTRAL PROCESSING UNIT) :**

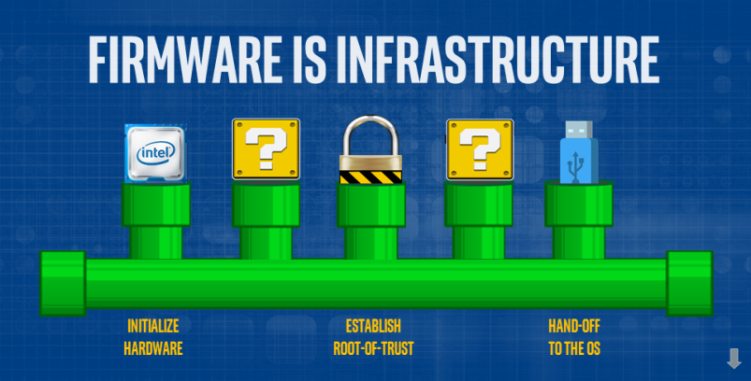
A **central processing unit** (**CPU**) is an important part of every computer. The CPU sends signals to control the other parts of the computer, almost like how a brain controls a body.The [**central processing unit (CPU)**](https://study.com/academy/lesson/central-processing-unit-cpu-parts-definition-function.html) of a computer is a piece of hardware that carries out the instructions of a computer program. It performs the basic arithmetical, logical, and input/output operations of a computer system. The CPU is like the brains of the computer.So let's say you press the letter 'k' on your keyboard and it appears on the screen - the CPU of your computer is what makes this possible So when you are looking at the specifications of a computer at your local electronics store, it typically refers to the CPU as the **processor**.



**FIRMWARE :**

Firmware is a software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

Firmware is data that is stored on a computer or other hardware device's read-only memory ([ROM](https://www.computerhope.com/jargon/r/rom.htm)) that provides instruction on how that device should operate. Unlike normal software, **firmware** cannot be changed or deleted by an [end-user](https://www.computerhope.com/jargon/e/enduser.htm) without the aid of special programs and remains on that device whether or not it's on or off.



**POWERSUPPLY :**

Short for **power supply** and sometimes abbreviated as **PSU**, which is short for **Power Supply Unit**. A **power supply** is an internal [hardware](https://www.computerhope.com/jargon/h/hardware.htm) component that supplies components in a [computer](https://www.computerhope.com/jargon/c/computer.htm) with power. The power supply converts a 110-115 or 220-230 volt alternating current ([AC](https://www.computerhope.com/jargon/a/ac.htm)) into a steady low-voltage direct current ([DC](https://www.computerhope.com/jargon/d/dc.htm)) usable by the computer and rated by the number of watts it generates. For example, the image to the right is an [Antec](https://www.computerhope.com/comp/antec.htm) True 330, a 330 [Watt](https://www.computerhope.com/jargon/w/watt.htm) power supply.

Below is a list of parts you may find on the back of the power supply.

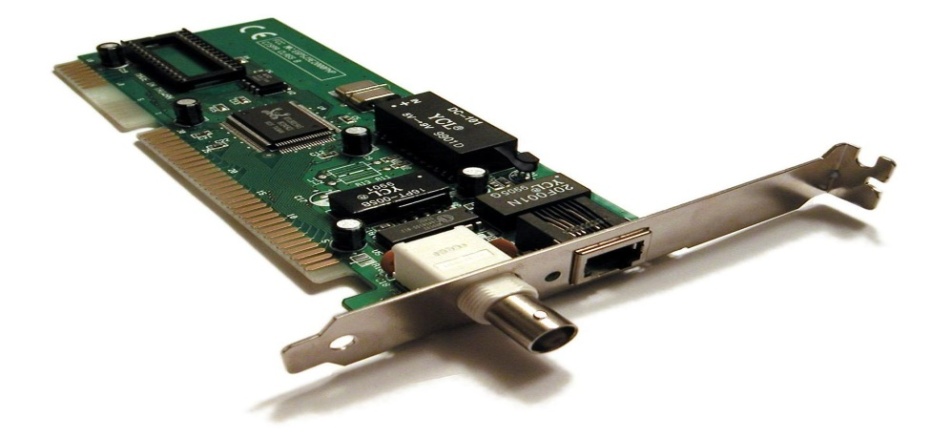
* A connection for the [power cord](https://www.computerhope.com/jargon/p/powecord.htm) to the computer.
* A fan opening to draw air out of the power supply.
* A red switch to change the power supply voltage.
* A [rocker switch](https://www.computerhope.com/jargon/r/rocker-switch.htm) to turn the power supply on and off.



**REMOVABLE MEDIA -**

NIC(NETWORK INTERFACE CARD) :

A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network. A network interface card provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology .



**CD(COMPACT DISK) :**

Compact discs are used to store data so that may be retrieved or executed at a later date. CDs can store software programs so that you may load them onto your computer. They save files for backup or transfer to another computer, as well as hold music to play in a CD player.



**DVD(DIGITAL VERSATILE DISK) :**

Short for **Digital Versatile Disc** or **Digital Video Disc**, a **DVD** or **DVD-ROM** is a disc capable of storing large amounts of data on one disc the size of a standard Compact Disc. **CD/DVD drives** were first sold in 1997. They are widely used for storing and viewing movies and other data. To play DVDs on a computer, you must have a DVD drive and a software DVD player. The picture to the right is an example of what a DVD movie may look like, which in this example is a picture of the Matrix DVD movie



INTERNAL STORAGE🡪

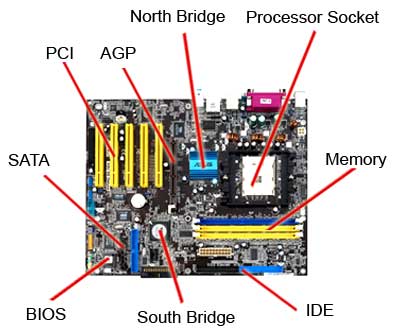
HARD DISK DRIVE (HDD):

A **hard disk drive** (**HDD**), **hard disk**, hard **drive** or fixed disk is a data storage device that uses magnetic storage to store and retrieve digitalinformation using one or more rigid rapidly rotating disks (platters) coated with magnetic material.



**MOTHERBOARD :**

A motherboard is the main printed circuit board (PCB) found in general purpose microcomputers and other expandable systems. It holds and allows communication between many of the crucial electronic components of a system, such as the central processing unit(CPU) and memory, and provides connectors for other peripherals. Unlike a backplane, a motherboard usually contains significant sub-systems such as the central processor, the chipset's input/output and memory controllers, interface connectors, and other components integrated for general purpose use.



* SOCKETS (or slots) in which one or more microprocessors may be installed. In the case of CPUs in ball grid arraypackages, such as the VIA C3, the CPU is directly soldered to the motherboard.
* A CHIPEST which forms an interface between the CPU's front-side bus, main memory, and peripheral buses.
* NON-VOLATILE MEMORY chips (usually Flash ROM in modern motherboards) containing the system's firmware or BIOS.
* A CLOCK GENERATOR which produces the system clock signal to synchronize the various component.

EXPERIMENT NO. 2

AIM-STUDY OF NETWORK DEVICES IN DETAIL

HUB :

A hub is a common connection point for [devices](http://www.webopedia.com/TERM/D/device.html) in a [network](http://www.webopedia.com/TERM/N/network.html). Hubs are commonly used to connect [segments](http://www.webopedia.com/TERM/S/segment.html) of a [LAN](http://www.webopedia.com/TERM/L/local_area_network_LAN.html). A hub contains multiple [ports](http://www.webopedia.com/TERM/P/port.html). When a [packet](http://www.webopedia.com/TERM/P/packet.html) arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hub works on Physical Layer. Logically it works Like**BUS Topology**But Look like **STAR Topology.**

Most hubs can detect basic network errors such as collisions, but having all information broadcast to multiple ports can be a security risk and cause bottlenecks. In the past, network hubs were popular because they were cheaper than a switch or router. Today, switches do not cost much more than a hub and are a much better solution for any network.



ETHERNET HUB :

A hub joins multiple computers (or other network devices) together to form a single network segment. On this network segment, all computers can communicate directly with each other

An **ethernet hub** is an electronic device that runs a computer network. It is a simple device and is easy to configure. A hub acts like a repeater: all data that arrives to one port is sent to all other ports (without looking at IP address for the data's destination). That means that all devices in this network will get all data.

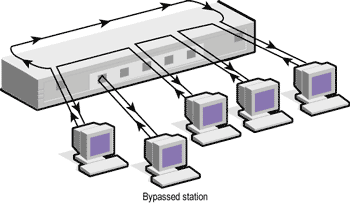
.

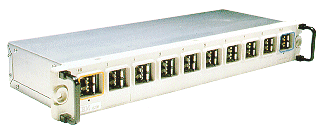
The number of [ports](https://www.lifewire.com/computer-port-usage-817366) an Ethernet hub supports also varies. Four- and five-port Ethernet hubs are most common in home networks, but eight- and 16-port hubs can be found in some home and small office environments. Hubs can be connected to each other to expand the total number of devices a hub network can support.Older Ethernet hubs were relatively large in size and sometimes noisy as they contained built-in fans for cooling the unit. Modern hub devices are much smaller, designed for mobility, and noiseless.



MULTISTATION ACCESS UNIT :

 A multistation access unit is a token-ring network device that physically connects network computers in a star topology while retaining the logical ring structure. One of the problems with the token-ring topology is that a single non-operating node can break the ring. The MAU solves this problem because it has the ability to short out non-operating nodes and maintain the ring structure. A MAU is a special type of hub.





SWITCHES :

A **network switch** (also called **switching hub**, **bridging hub**, officially **MAC bridge**) is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer(layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

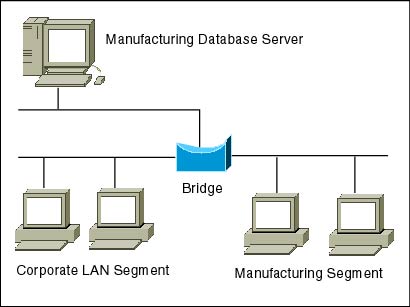


BRIDGES :

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

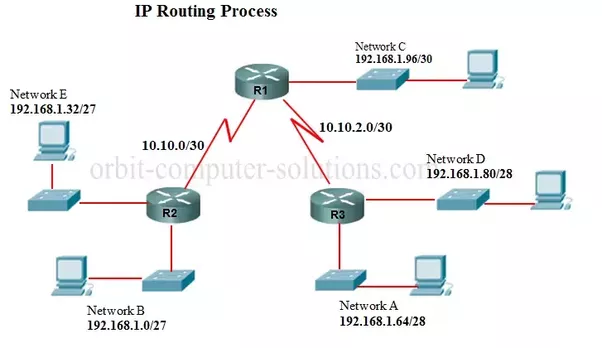
Bridges are also known as Layer 2 switches.



ROUTERS:

A **router** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another router through the networks that constitute an internetworkuntil it reaches its destination node.

A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

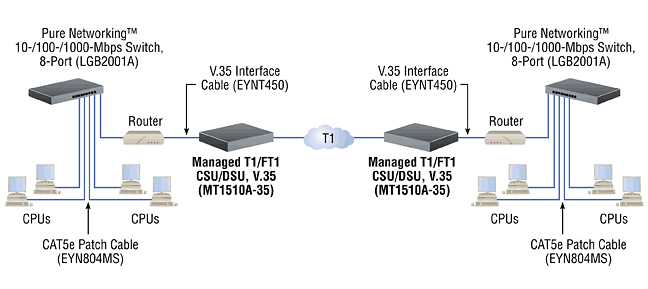


When multiple routers are used in interconnected networks, the routers can exchange information about destination addresses using a routing protocol. Each router builds up a routing table listing the preferred routes between any two systems on the interconnected networks.



CSU/DSU(CHANNEL SERVICE UNIT/DATA SERVICE UNIT) :

A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts a digital data [frame](http://searchnetworking.techtarget.com/definition/frame) from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa. For example, if you have a Web business from your own home and have leased a digital line (perhaps a T-1 or fractional T-1 line) to a phone company or a [gateway](http://searchnetworking.techtarget.com/definition/gateway) at an Internet service provider, you have a CSU/DSU at your end and the phone company or gateway host has a CSU/DSU at its end.



A **CSU/DSU**  is a digital-interface device used to connect data terminal equipment (DTE), such as a router, to a digital circuit, such as a Digital Signal 1 (DS1) T1 line. The CSU/DSU implements two different functions. The channel service unit (CSU) is responsible for the connection to the telecommunication network, while the data service unit (DSU) is responsible for managing the interface with the DTE.

Network protocols :

Network protocols incorporate all the processes, requirements and constraints of initiating and accomplishing communication between computers, servers, routers and other network enabled devices. Network protocols must be confirmed and installed by the sender and receiver to ensure network/data communication and apply to software and hardware nodes that communicate on a network. There are several broad types of networking protocols, including: Network communication protocols: Basic data communication protocols, such as TCP/IP and HTTPNetwork security protocols:

ISDN ADAPTERS :

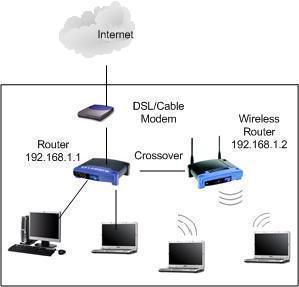
**Integrated Services Digital Network** (**ISDN**) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).



WIRELESS ACCESS POINT (WAP) :

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.



MODEMS :

A **modem** (**mo**dulator–**dem**odulator) is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light-emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.



Modems are generally classified by the maximum amount of data they can send in a given unit of time, usually expressed in bits per second (symbol **bit(s)**, sometimes abbreviated "bps"), or bytes per second (symbol **B(s)**).

FIREWALLS :

 A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Firewalls are often categorized as either **network firewalls** or **host-based firewalls**. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

### Packet filtering firewall :

This type of firewall has a list of firewall security rules which can block traffic based on IP protocol, IP address and/or port number. Under this firewall management program, all web traffic will be allowed, including web-based attacks. In this situation, you need to have intrusion prevention, in addition to firewall security, in order to differentiate between good web traffic (simple web requests from people browsing your website) and bad web traffic (people attacking your website).

### Stateful firewall :

This is similar to a packet filtering firewall, but it is more intelligent about keeping track of active connections, so you can define firewall management rules such as "only allow packets into the network that are part of an already established outbound connection." You have solved the established connection issue described above, but you still can't tell the difference between "good" and "bad" web traffic. You need intrusion prevention to detect and block web attacks.

### Deep packet inspection firewall :

An application firewall actually examines the data in the packet, and can therefore look at application layer attacks. This kind of firewall security is similar to intrusion prevention technology, and therefore may be able to provide some of the same functionality.

Application-aware firewall :

Similar to deep packet inspection, except that the firewall understands certain protocols and can parse them, so that signatures or rules can specifically address certain fields in the protocol. The flexibility of this approach to computer firewall protection is great and permits the signatures or rules to be both specific and comprehensive. There are no specific drawbacks to this approach to firewall security as generally it will yield improvements over a standard "deep packet inspection" approach. However, some actual attacks may be overlooked (false negatives) because the firewall security parsing routines are not robust enough to handle variations in real-world traffic.

### Application proxy firewall :

An application proxy acts as an intermediary for certain application traffic (such as HTTP or web traffic), intercepting all requests and validating them before passing them along. Again an application proxy firewall is similar to certain kinds of intrusion prevention. The implementation of a full application proxy is, however, quite difficult, and each proxy can only handle one protocol (e.g. web or incoming email).

For an application proxy firewall to be effective as computer firewall protection, it has to be able to understand the protocol completely and to enforce blocking on violations of the protocol. Because implementations of the protocol being examined often do not follow a protocol correctly, or because implementers add their own extensions to a protocol, this can result in the proxy blocking valid traffic (false positives). Because of these kinds of problems, end users will often not enable these technologies.

EXPERIMENT NO. 3

AIM : CONNECT COMPUTERS IN LAN

You can connect the computers to one another using a crossover Ethernet cable. After connecting your computers together with an Ethernet cable, you will be required to modify the network settings on one of the computers to establish the cable connection. You will then have the ability to transfer or share files, and play network games between both computers.



STEP-1 : CONNECTIONS

* **Verify that you have a crossover Ethernet cable.** Examine the wire color patterns at each end of the Ethernet cable to determine whether or not the colors match up. A crossover Ethernet cable will have color patterns that do not match up; whereas on standard cables, the color patterns will match up to one another identically on each end.



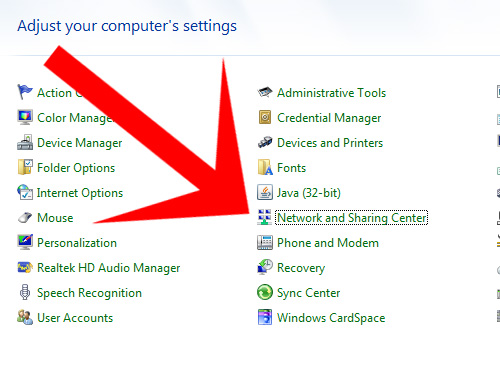
* **Plug each end of the Ethernet cable into an Ethernet network port on each computer to connect the computers together with the cable.**



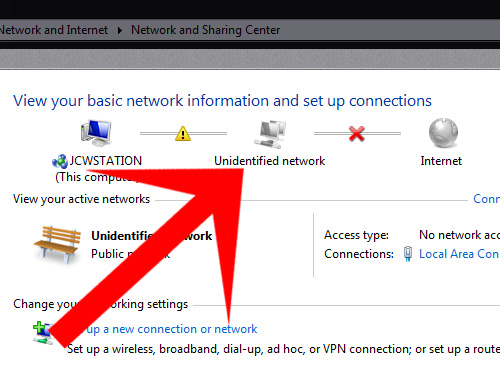
**STEP-2 : COMPUTER SETTING**

* **Click on the "Start" menu.**
* **Select "Control Panel," then type "network" into the search box provided to you within Control Panel.**
* **Select "Network and Sharing Center" from the options displayed in**

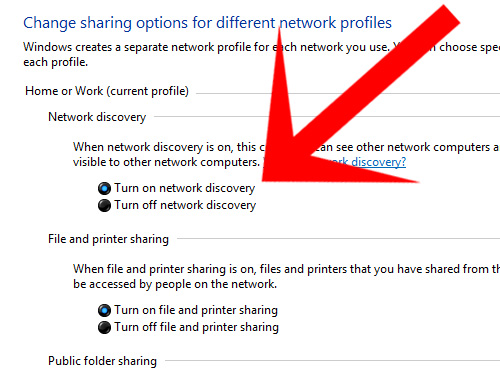
**the window.**



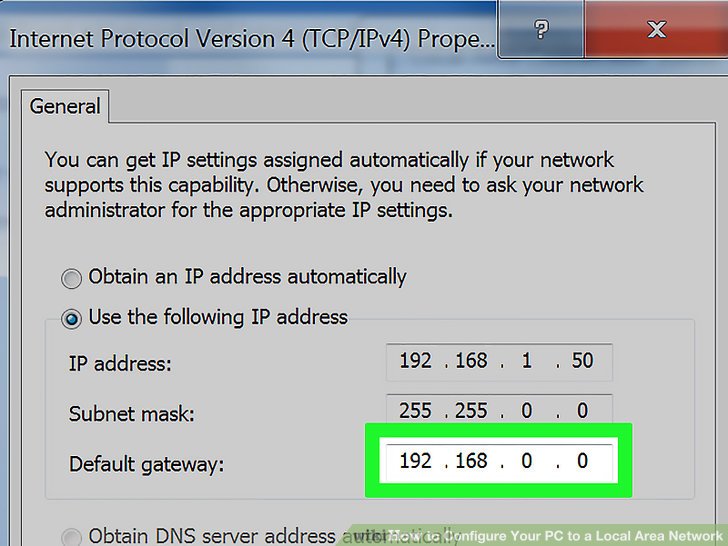
* **Select and open the icon labeled "Unidentified network" from the network map at the top of the Network and Sharing Center window.**



* **Click on the message that prompts you to change the network discovery and file sharing settings, then click on the option that reads, "Turn on network discovery and file sharing”.**



* **Type the administrator password for the computer if prompted to do so, then press "Enter" on your keyboard.**



EXPERIMENT NO. 4

AIM : STUDY OF CCTV SURVEILLANCE

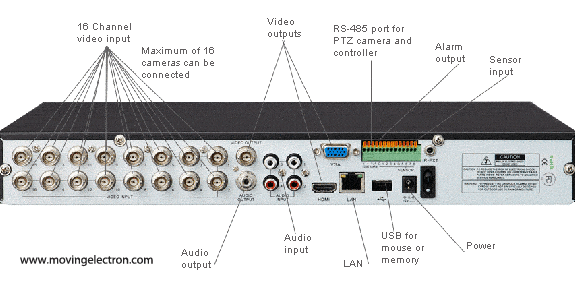
* Closed Circuit Television (CCTV) is a system where the circuit in which the video is transmitted is closed and all the elements (camera, display monitors, recording devices) are directly connected. This is unlike broadcast television where any receiver that is correctly tuned can pick up and display or store the signal.
* The most common use of CCTV is in security camera systems. They’ve been found for years in areas like large retail shops, banks, and government institutions.
* Any camera that broadcasts a signal can be attached to a CCTV system, whether it’s wired or wireless, but they are most often associated with high-end surveillance cameras.



DVR(DIGITAL VIDEO RECORDER) :

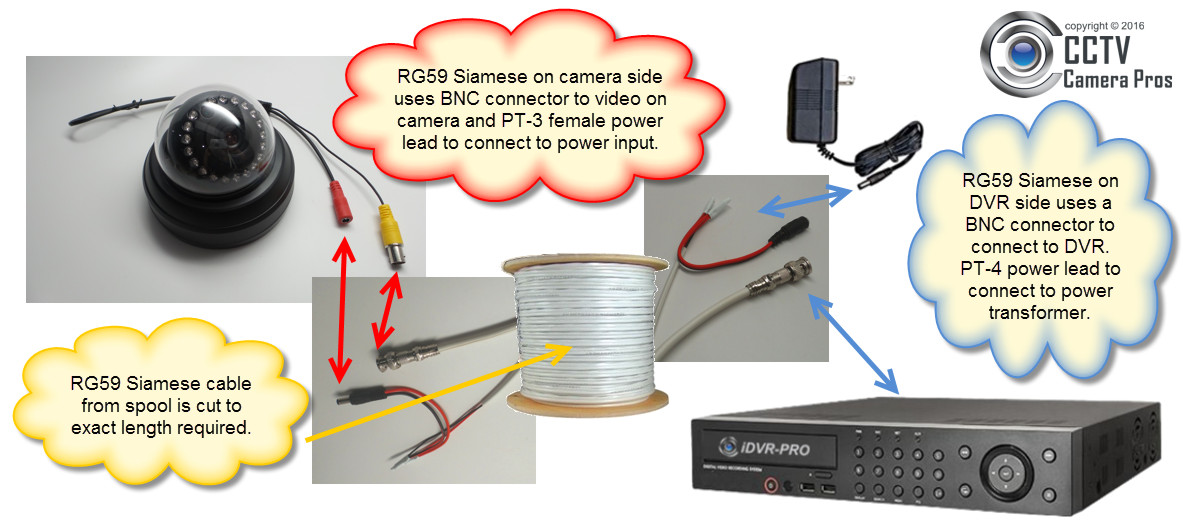
* **DVR** forms the central hub of your surveillance system.
* **DVR** is an electronic device that records video in a digital format to a disk drive, USB flash drive, SD memory card, SSD or other local or networked mass storagedevice.
* A **CCTV** digital video recorder (or “**DVR**” for short) is essentially a computer that saves security video images to a hard drive. Most security cameras in use today capture an analog picture. The **DVR** converts the analog signal to digital and then compresses it.





CONNECTIONS :

* Connect the plug and play cable to the DVR.
* The male BNC connector on the cable very simple pushes and twists on to the female BNC input on the back of the DVR.
* Grab the other end of the cable.
* Attach the BNC connector to the security camera. Again, it simply pushes and twists on.
* Attach the power side of the cable to the power input of the camera. This simple pushes on.
* Attach the power supply plug of the security camera to the other end of the plug and play cable.
* Last, plug the power supply into a standard power outlet.



PORT FORWARDING :

Port forwarding is essential to making your security DVR accessible from online using either your computer or mobile device. It is a configuration setting in your router that must be set properly in order to view your security camera system from the internet.

STEPS :

### 1🡪Determine Router and Computer IP Address, and

### Router Password

**Information Required :**

* **Gateway IP Address:** The default IP address of your router; your computer and DVR must be connected to this gateway and have an IP address that conforms to this Gateway IP.
* **External IP Address:** The IP address for your internet connection provided by your ISP. This is your IP address on the Internet. All of the computers on your local network are behind this IP address.
* **DVR IP address:** The IP address of your DVR. The default IP address for DVRs and NVRs purchased from CCTV Camera World is 192.168.1.108.
* **Ports that need to be port forwarded:** check within the DVR's network settings to confirm the values for ports it uses. For our recorders, as explained above, the default ports are 80, and 37777.

## 2🡪Finding your DVR's IP address and Ports

* Look under the SETTING section and choose the option NETWORK.
* Choose the TCP/IP option to bring up the networking menu of interest to us.

On the TCP/IP page you will see what your DVR’s IP address is set to. More often than not, the default is 192.168.1.108. If your Gateway IP Address from Step 1 above was 192.168.1.1, you can leave the DVR ip address as the default value. You should only change it if it is not following the same IP address scheme as your router. If the router’s IP (default gateway) is 10.1.10.1 then you must change the DVR ip to reflect this. Something like 10.1.10.108 will suffice.

* choose the tab on the left called “Connection.”



Here you will find the active port numbers assigned for these types of services. By default these should be **port 80 for HTTP**and **port 3777 for TCP**. Leave these as they are but note where they are located in case you need to change them when configuring port forwarding. If you have made any changes on this, click apply and save when finished.

## 3🡪Creating Port Forwarding Rules in your Router

* **Login to your router**
* **Find the port forwarding menu**

In the left hand column we find a link for Virtual Servers, click on it.

* **Create the port forward rules**

Click ADD to make a new port rule, which should bring up a input box similar to the one

Below.

Now we will make the first port rule. We will start with port 80. Here's what you should enter

For each field.

***Description*** - This is simply the name for the port rule you are creating. Make it something obvious in case you need to change it later like “port 80” or “DVR 80.”

***Inbound Port*** - This stands for the ports on the internet side of the router that you would like to open. We are opening only one port at a time, and will not enter a range. Enter 80 for both the beginning and end.

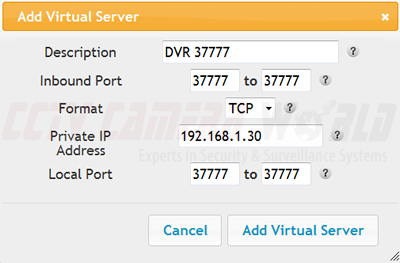
***Format*** - This is the protocol or port type. There should be three choices for port types: 1) TCP  2) UDP  3) Both. Choose TCP for ports 80 and 37777.

***Private IP Address*** - This refers to the IP address of the device you want to forward or point this rule to, which in our case is the IP of the DVR. The ip address of our DVR is 192.168.1.30.

***Local Port*** - This is the port number on the DVR that we want to forward the inbound port to. In our case they should be the same as Inbound Port, and the same for the beginning and end of the Local Port range. So enter 80.

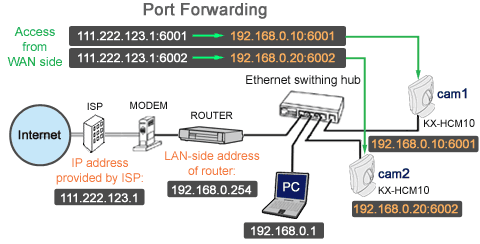
Once all of this information is filled out, click Add Virtual Server to finalize this port rule.

Now your first rule for port 80 is created. Follow these steps again to add the other port rule for port 37777. Add it exactly in the same way, but substitute 37777 for wherever you added 80.



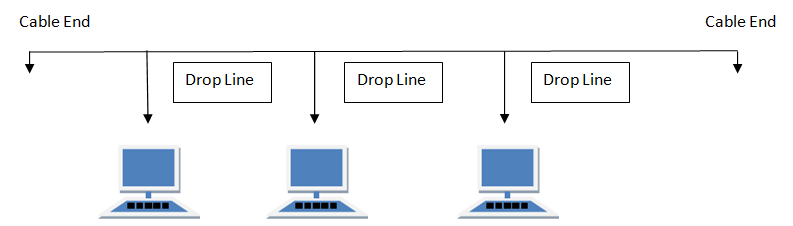
## 4🡪 Confirm Port Forwarding Rules are working

If your port rules were created properly, you should be ready to access your DVR from an external source. One last thing you should do to make sure your rules were created properly is to do a port scan on your internet connection to confirm the ports are indeed open.



EXPERIMENT NO. 5

**AIM: CONFIGURE NETWORK TOPOLOGIES**

~~~~

**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**

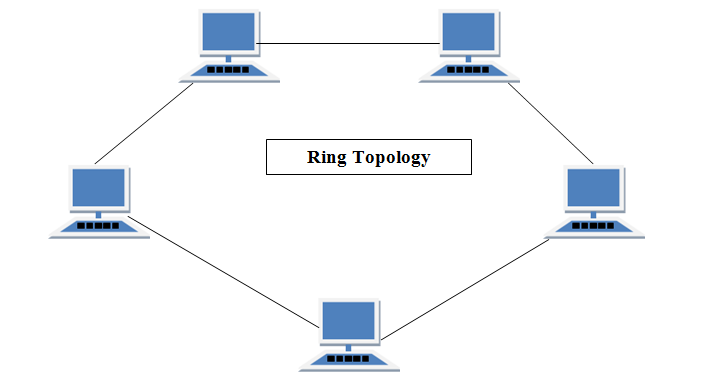
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

**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.



**Features of Ring Topology**

1. A number of repeaters are used for Ring topology with large number of nodes to prevent data loss in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

**Advantages of Ring Topology**

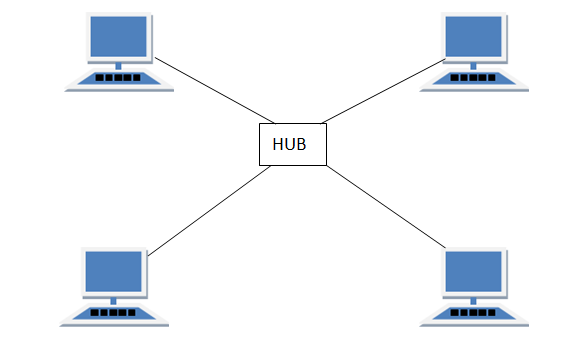
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

**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.



**Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Hub 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 fails 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. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

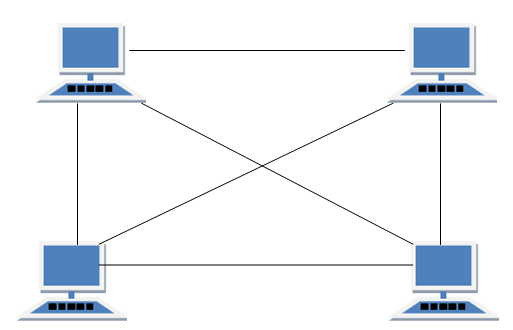
1. Routing
2. Flooding

**MESH Topology: Routing**

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

**MESH Topology: Flooding**

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



**Features of Mesh Topology**

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

**Advantages of Mesh Topology**

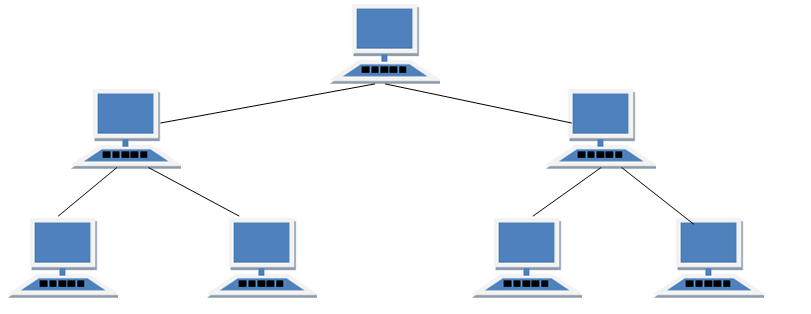
1. Each connection can carry its own data load.
2. Fault is diagnosed easily.
3. Provides security and privacy.

**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.



**Features of Tree Topology**

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

**Advantages of Tree Topology**

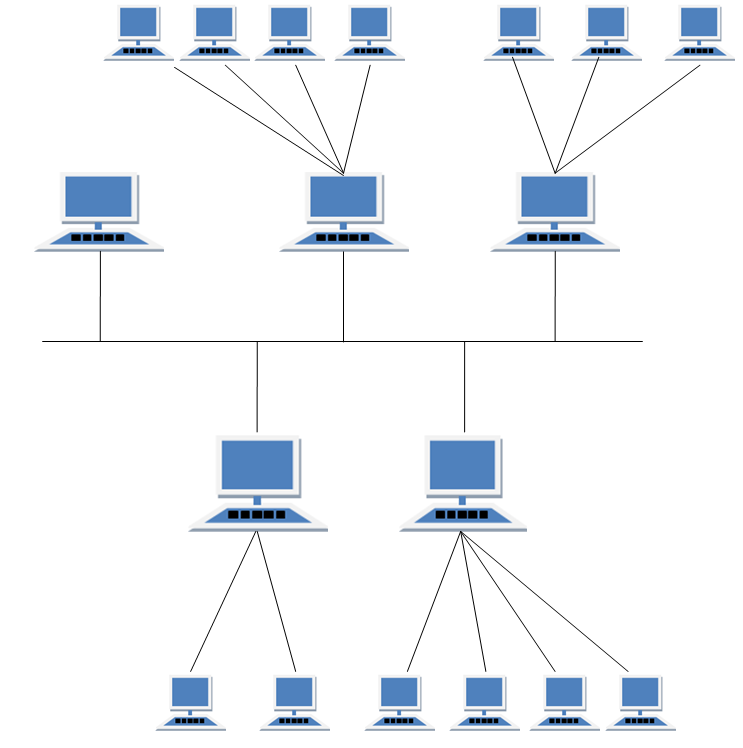
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

**Disadvantages of Tree Topology**

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

**HYBRID Topology**

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



**Features of Hybrid Topology**

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

**Advantages of Hybrid Topology**

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

**Disadvantages of Hybrid Topology**

1. Complex in design.
2. Costly.

EXPERIMENT NO. 6

AIM : STUDY OF BIT STUFFING IN FRAMES

Bit stuffing is the process of inserting non information bits into data to break up bit patterns to affect the synchronous transmission of information. It is widely used in network and communication protocols, in which bit stuffing is a required part of the transmission process. Bit stuffing is commonly used to bring bit streams up to a common transmission rate or to fill frames. Bit stuffing is also used for run-length limited coding.

In order to fill bit frames, the position where the new bits are stuffed is communicated to the receiving end of the data link. The receiver removes the extra bits to return the bit streams to their original bit rate. This is used when a communication protocol requires a fixed frame size. Bits are inserted to make the frame size equal to the defined frame size.  
  
Bit stuffing also works to limit the number of consecutive bits of the same value included in the transmitted data for run-length limited coding. This procedure includes a bit of the opposite value after the maximum allowed number of consecutive bits of the same value. For instance, if a number of zero bits are transmitted consecutively, the receiving end loses synchronization because a lot of time has passed without voltage sensing. Using bit stuffing, sets of bits beginning with the number one are stuffed into streams of zeros at specific intervals. The receiver does not require any extra information regarding the bit location when the extra bits are removed. Such bit stuffing is done to ensure reliable data transmission and ensure that transmissions start and end at the right places, among other purposes.

Bit Stuffing Program

Bit stuffing is a process of inserting an extra bit as 0, once the frame sequence encountered 5 consecutive 1's.

#include<stdio.h>

#include<conio.h>

#include<string.h>

voidmain()

{

    inta[20],b[30],i,j,k,count,n;

    printf("Enter frame size :");

    scanf("%d",&n);

    printf("Enter the frame in the form of 0 and 1 :");

    for(i=0; i<n; i++)

        scanf("%d",&a[i]);

    i=0;

    count=1;

    j=0;

    while(i<n)

    {

        if(a[i]==1)

        {

            b[j]=a[i];

            for(k=i+1; a[k]==1 && k<n && count<5; k++)

            {

                j++;

                b[j]=a[k];

                count++;

                if(count==5)

                {

                    j++;

                    b[j]=0;

                }

                i=k;

            }

        }

        else

        {

            b[j]=a[i];

        }

        i++;

        j++;

    }

    printf("After Bit Stuffing :");

    for(i=0; i<j; i++)

        printf("%d",b[i]);

    getch();

}

OUTPUT for BIT STUFFING:

Enter frame size :12

Enter the frame in the form of 0 and 1: 0 1 0 1 1 1 1 1 1 0 0 1

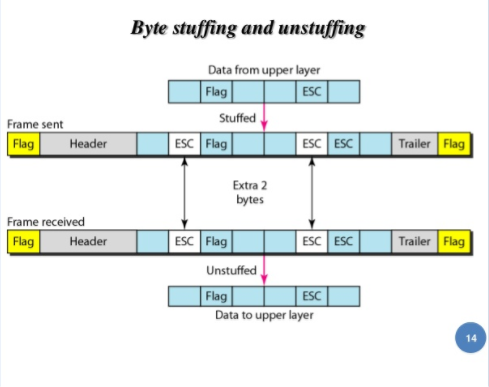
After Bit Stuffing: 0101111101001

EXPERIMENT NO. 7

AIM: STUDY OF BYTE STUFFING OF FRAMES

BYTE STIUFFING:

Byte stuffing is a process that transforms a sequence of data bytes that may contain 'illegal' or 'reserved' values (such as packet delimiter) into a potentially longer sequence that contains no occurrences of those values. The extra length of the transformed sequence is typically referred to as the overhead of the algorithm. The COBS algorithm tightly bounds the worst-case overhead, limiting it to a minimum of one byte and a maximum of ⌈n/254⌉ bytes (one byte in 254, rounded up). Consequently, the time to transmit the encoded byte sequence is highly predictable, which makes COBS useful for real-time applications in which jitter may be problematic. The algorithm is computationally inexpensive and its average overhead is low compared to other unambiguous framing algorithms.



**Packet framing and stuffing:**

When packetized data is sent over any serial medium, some protocol is required to demarcate packet boundaries. This is done by using a framing marker, a special bit-sequence or character value that indicates where the boundaries between packets fall. Data stuffing is the process that transforms the packet data before transmission to eliminate all occurrences of the framing marker, so that when the receiver detects a marker, it can be certain that the marker indicates a boundary between packets.

COBS transforms an arbitrary string of bytes in the range [0,255] into bytes in the range [1,255]. Having eliminated all zero bytes from the data, a zero byte can now be used to unambiguously mark the end of the transformed data. This is done by appending a zero byte to the transformed data, thus forming a packet consisting of the COBS-encoded data (the payload) to unambiguously mark the end of the packet.

(Any other byte value may be reserved as the packet delimiter, but using zero simplifies the description.)

Consistent Overhead Byte Stuffing (COBS) encoding process

There are two equivalent ways to describe the COBS encoding process:

**Prefixed block description:**

To encode some bytes, first append a zero byte, then break them into groups of either 254 non-zero bytes, or 0–253 non-zero bytes followed by a zero byte. Because of the appended zero byte, this is always possible.

Encode each group by deleting the trailing zero byte (if any) and prepending the number of non-zero bytes, plus one. Thus, each encoded group is the same size as the original, except that 254 non-zero bytes are encoded into 255 bytes by prepending a byte of 255.

As a special exception, if a packet ends with a group of 254 non-zero bytes, it is not necessary to add the trailing zero byte. This saves one byte in some situations.

**Linked list description:**

First, insert a zero byte at the beginning of the packet, and after every run of 254 non-zero bytes. This encoding is obviously reversible. It is not necessary to insert a zero byte at the end of the packet if it happens to end with exactly 254 non-zero bytes.

Second, replace each zero byte with the offset to the next zero byte, or the end of the packet. Because of the extra zeros added in the first step, each offset is guaranteed to be at most 255.

**Encoding examples:**

These examples show how various data sequences would be encoded by the COBS algorithm. In the examples, all bytes are expressed as hexadecimal values, and encoded data is shown with text formatting to illustrate various features:

Bold indicates a data byte which has not been altered by encoding. All non-zero data bytes remain unaltered.

Green indicates a zero data byte that was altered by encoding. All zero data bytes are replaced during encoding by the offset to the following zero byte (i.e. one plus the number of non-zero bytes that follow). It is effectively a pointer to the next packet byte that requires interpretation: if the addressed byte is non-zero then it is the following group header byte zero data byte that points to the next byte requiring interpretation; if the addressed byte is zero then it is the end of packet.

Red is an overhead byte which is also a group header byte containing an offset to a following group, but does not correspond to a data byte. These appear in two places: at the beginning of every encoded packet, and after every group of 254 non-zero bytes.

A blue zero byte appears at the end of every packet to indicate end-of-packet to the data receiver. This packet delimiter byte is not part of COBS proper; it is an additional framing byte that is appended to the encoded output.

**Example Unencoded data (hex) Encoded with COBS (hex)**

1 00 01 01 00

2 00 00 01 01 01 00

3 11 22 00 33 03 11 22 02 33 00

4 11 22 33 44 05 11 22 33 44 00

5 11 00 00 00 02 11 01 01 01 00

6 01 02 03 ... FD FE FF 01 02 03 ... FD FE 00

7 00 01 02 ... FC FD FE 01 FF 01 02 ... FC FD FE 00

8 01 02 03 ... FD FE FF FF 01 02 03 ... FD FE 02 FF 00

9 02 03 04 ... FE FF 00 FF 02 03 04 ... FE FF 01 01 00

10 03 04 05 ... FF 00 01 FE 03 04 05 ... FF 02 01 00

EXPERIMENT NO. 8

AIM : STUDY OF CHARACTER STUFFING IN FRAMES

CHARACTER STUFFING :

Although using characters to mark the beginning and end of each frame has advantages, mostcomputer networkscannot afford to reserve characters for use by the network. Instead, the network permits anapplicationto transfer arbitrary data values across the network. In particular, an application may choose to send datathat contains one or more occurrences of characters like soh and eot that are used for framing. Ingeneral, to distinguish between data being sent and control information such as frame delimiters, networksystemsarrange for the sending side to change the data slightly before it is sent, and then arrange for thereceiving side to restore the original data before passing it to the receiving application.

Thus, although applications using the network can transfer arbitrary data, the network system never confuses data withcontrol information. Because network systems usually insert bits or bytes to changedata for transmission, the technique is known as data stuffing. The terms character stuffing and bytestuffing refer to data stuffing used with character orientedhardware, and bit stuffing which is morecommon, refers to data stuffing used with bit oriented hardware. To implement byte stuffing, a sender must scan an entire data block and perform the mapping before any data is sent. Byte stuffing can solvethe problem by reserving a third character to mark occurrences of special characters in the data.

Use reserved characters to indicate the start and end of a frame. For instance, use the two-character sequence DLE STX (Data-Link Escape, Start of TeXt) to signal the beginning of a frame, and thesequence DLE ETX (End of TeXt) to flag the frame's end.

Problem: What happens if the two-character sequence DLE ETX happens to appear in the frame itself?

Solution: Use character stuffing; within the frame, replace every occurrence of DLE with the two-character sequence DLE DLE. The receiver reverses the processes, replacing every occurrence of DLE DLE with a single DLE.

Example: If the frame contained ``A B DLE D E DLE'', the characters transmitted over the channel wouldbe ``DLE STX A B DLE DLE D E DLE DLE DLE ETX''.

Disadvantage: character is the smallest unit that can be operated on; not all architectures are byteoriented.

Character Stuffing Program

#include<stdio.h>

#include<string.h>

main()

{

char a[30], fs[50] = " ", t[3], sd, ed, x[3], s[3], d[3], y[3];

int i, j, p = 0, q = 0;

clrscr();

printf("Enter characters to be stuffed:");

scanf("%s", a);

printf("\nEnter a character that represents starting delimiter:");

scanf(" %c", &sd);

printf("\nEnter a character that represents ending delimiter:");

scanf(" %c", &ed);

x[0] = s[0] = s[1] = sd;

x[1] = s[2] = '\0';

y[0] = d[0] = d[1] = ed;

d[2] = y[1] = '\0';

strcat(fs, x);

for(i = 0; i<strlen(a); i++)

{

t[0] = a[i];

t[1] = '\0';

if(t[0] == sd)

strcat(fs, s);

elseif(t[0] == ed)

strcat(fs, d);

else

strcat(fs, t);

}

strcat(fs, y);

printf("\n After stuffing:%s", fs);

getch();

}

**Output:-**

Enter characters to be stuffed: goodday

Enter a character that represents starting delimiter: d

Enter a character that represents ending delimiter: g

After stuffing: dggooddddayg.

EXPERIMENT NO. 9

AIM : STUDY OF CYCLIC REDUNDANCY CHECK

Cyclic Redundancy Check (CRC) An error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRe is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.

A CRC is derived using a more complex algorithm than the simple CHECKSUM, involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial.

• CRC is more powerful than VRC and LRC in detecting errors.

• It is not based on binary addition like VRC and LRC. Rather it is based on binary division.

• At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC.

• The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit.

• The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor i.e. remainder becomes zero.

At the destination, the incoming data unit i.e. data + CRC is divided by the same number (predetermined binary divisor).

• If the remainder after division is zero then there is no error in the data unit & receiver accepts it.

• If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected.

• This technique is more powerful than the parity check and checksum error detection.

• CRC is based on binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of a data unit such as byte.

Requirements of CRC :

A CRC will be valid if and only if it satisfies the following requirements:

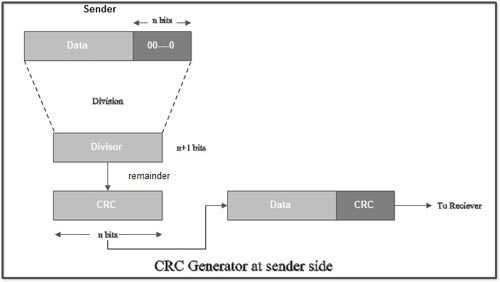
1. It should have exactly one less bit than divisor.

2. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

**The various steps followed in the CRC method are**

1. A string of n as is appended to the data unit. The length of predetermined divisor is n+ 1.

2. The newly formed data unit *i.e.*original data + string of n as are divided by the divisor using binary division and remainder is obtained. This remainder is called CRC.

[](http://ecomputernotes.com/images/CRC-generator-at-sender-side.jpg)

3. Now, string of n Os appended to data unit is replaced by the CRC remainder (which is also of n bit).

4. The data unit + CRC is then transmitted to receiver.

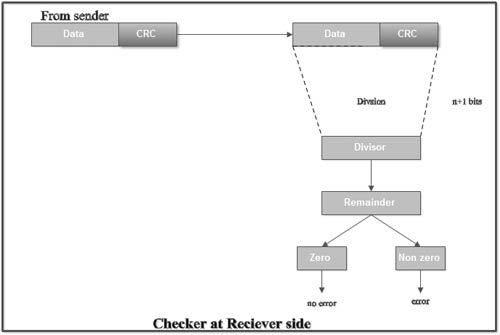
5. The receiver on receiving it divides data unit + CRC by the same divisor & checks the remainder.

6. If the remainder of division is zero, receiver assumes that there is no error in data and it accepts it.

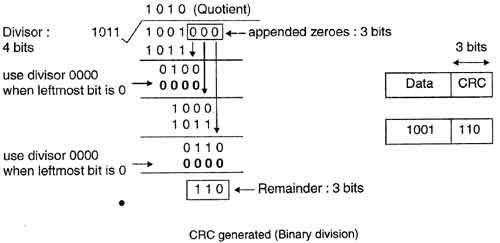
7. If remainder is non-zero then there is an error in data and receiver rejects it.

• For example, if data to be transmitted is 1001 and predetermined divisor is 1011. The procedure given below is used:

1. String of 3 zeroes is appended to 1011 as divisor is of 4 bits. Now newly formed data is 1011000.

[](http://ecomputernotes.com/images/CRC-checker-at-receiver-side.jpg)

1. Data unit 1011000 is divided by 1011.

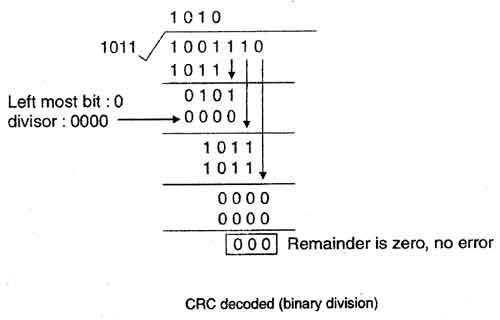
[](http://ecomputernotes.com/images/CRC-generated-Binary-division.jpg)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.

[](http://ecomputernotes.com/images/CRC-decoded-Binary-division.jpg)

• CRC can detect all the burst errors that affect an odd number of bits.

• The probability of error detection and the types of detectable errors depends on the choice of divisor.

• Thus two major requirement of CRC are:

(a) CRC should have exactly one bit less than divisor.

(b) Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.