NETWORK FUNCTIONS

Following are the essential network functions:

1) Terminal:
The main function of the network is to transfer the information between a source and a destination. The source and the destination are known as the terminals which are attached within the network.

2) Transmission:
The process of data transfer which involve the transfer of the single block of information or the transfer of a stream of information. The network must be able to provide connectivity in sense of providing a mean for the transfer of information among the users. This basic capability is provided by transmission system such as copper wire, cables, optical fiber, infrared, etc.

3) Information representation:
The information is represented in the form of bits, characters, analog or digital signal, voice signals, etc.

4) Switching:
Switching transfers the information flow from one transmission line to other.

5) Routing and forwarding:
Routing decides the best known path to transfer data from one point to another and forwarding help forward data on that path.

6) Addressing:
It is required to identify which network input is to be connected to which network output. There are two types of addressing:

a) Hierarchical addressing for WAN
b) Flat addressing for LAN

7) Traffic and congestion control:
The traffic control is necessary for the smooth flow of the information through the network and when congestion occurs inside the network the network should react by applying the congestion or overload control mechanism.

8) Network management:
it includes the monitoring of the network, detecting and recovering the faults, configure the network resources, maintaining the information and providing security by controlling access to the information flow in the network.

Basic Concepts Of Networking

How Data Is Transmitted From One Device to Another: It is important to understand the relationship between communicating devices. Five general concepts provide the basis for this relationship:

1. Line Configuration
2. Topology
3. Transmission Mode
4. Categories of Networks
5. Internetworks

1. **LINE CONFIGURATION** refers to the way two or more communication devices attach to a link. A link is the physical communication pathway that transfers data from one device to another. It is of two types:

(i) Point to Point
(ii) Multipoint

(i) **Point to Point**: It provides a dedicated link between two devices. The entire capacity of the channel is reserved for transmission between these two devices. Most point to point line configurations use an actual length of wire or cable to connect the two ends but microwave & satellite links are also used.

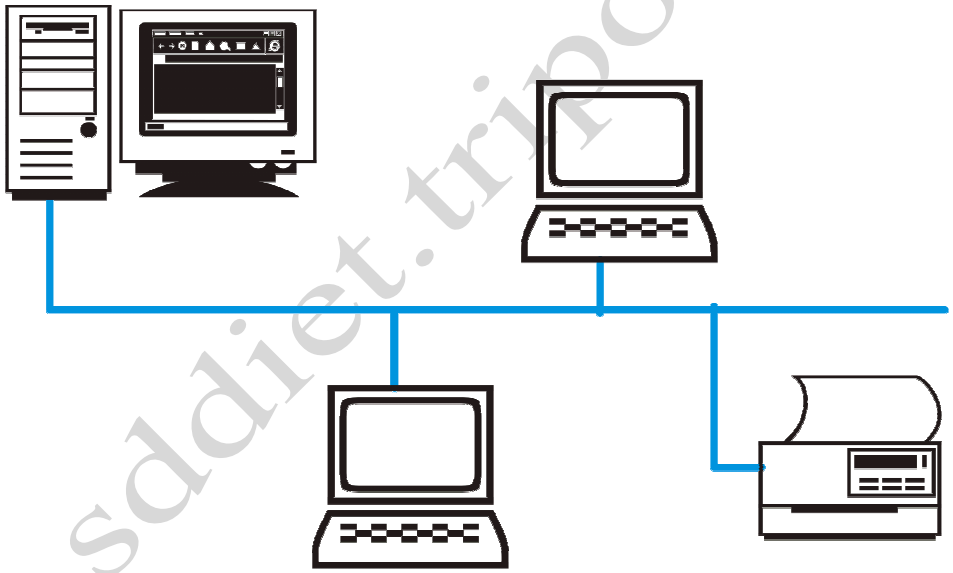
P2P Network: consists of many connections between individual parts of machine. To go from source to destination, a packet must have to first visit one or more intermediate machines. P2P transmission with one sender and one receiver is also called unicasting.

There are 3 types of P2P networks:

a) **Unicast Network**: as explained above
b) **Broadcast Network**: has a single common channel that is shared by all the machines on the network. Short messages called packets sent by any machine are received by all others. An address field within the packet specifies its destination. Upon receiving a packet, machine checks the address field. If the packet is not for that particular machine, it just ignores it. So broadcast system allows the possibility of adding a packet to all destinations. This mode of operation is called broadcasting.

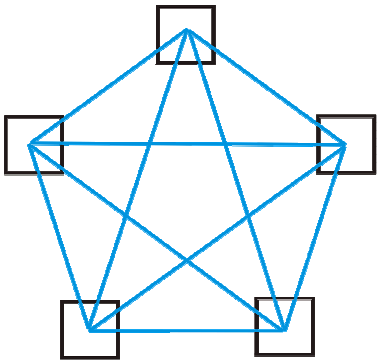
c) **Multi Network**: It is made up of a number of broadcast networks.

(ii) **Multipoint**: it is one in which more than two specific devices share a single link.



2. **TOPOLOGY**: the term topology refers to the way a network is laid out either physically or logically. The topology of a network is representation of the relationship of all the links and linking devices to each other. There are 5 basic topologies:

i. Mesh: in this 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.



Advantages:

(a) **Dedicated link** guarantees that each connection carries its own data load that eliminates the traffic problem.

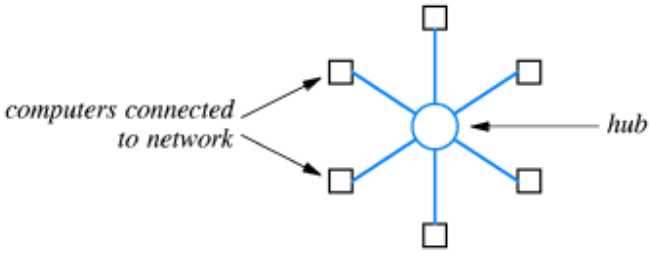
(b) It is **robust**. If one link becomes unusable, it does not affect the work of other devices.

(c) It provides **privacy** and **security**.

Disadvantage:

Long cables and many I/O ports are required which make the **circuit** very **complicated**.

ii. Star: in this topology, each device has a dedicated point to point link only to a central controller called a hub. The devices are not directly linked to each other. There is no direct traffic between devices. The controller acts as an exchange.



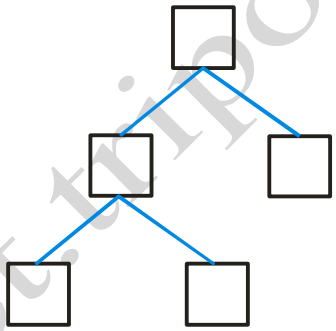
Advantages:

(a) Less expensive as compared to mesh.

(b) Each device needs only one link one I/O port to connect it to any number of others.
(c) Robustness. If one link fails, only that link is affected.

Disadvantages:
(a) Hub failure
(b) More cabling as compared to other topologies.

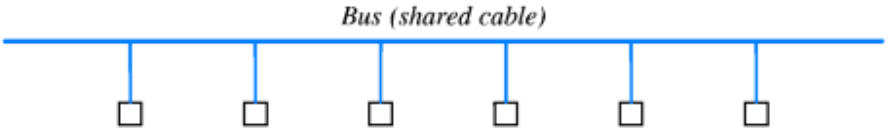
iii. Tree: it is a variation of a star topology. As in star, nodes in a tree are linked to a central hub. In this not every device plugs directly into the central hub. The majority of devices connect to a secondary hub that is in turn connected to the central hub. It is called active hub. The secondary hubs maybe active or passive hubs. A passive hub provides a simple physical connection between the attached devices.



Advantage:
Large number of devices can be connected to a single central hub.

Disadvantage:
Hub failure.

iv. Bus: this is a multipoint topology. In this, one cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by a connection between the device and the main cable.



Advantages:

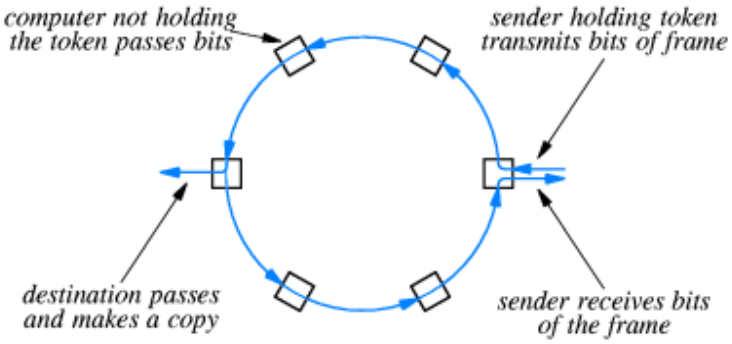
(a) Easy to install.

(b) Less cabling id required.

Disadvantage:

Fault or break in bus cable stops all transmission.

v. Ring: Each device has a dedicated point to point line configuration only with two devices on either side of it. Signal is passed along the ring in one direction from device to device until it reaches its destination.



Advantages:

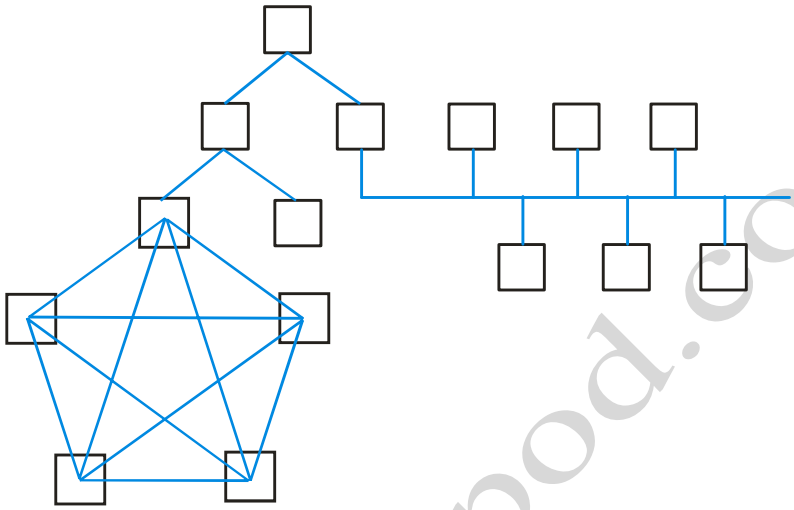
(a) Easy to install.

(b) Each device is linked only to its immediate neighbor. To add or delete a device requires moving only two connections.

Disadvantage:

Unidirectional flow of data. So if there is a break in link, it disables the entire network.

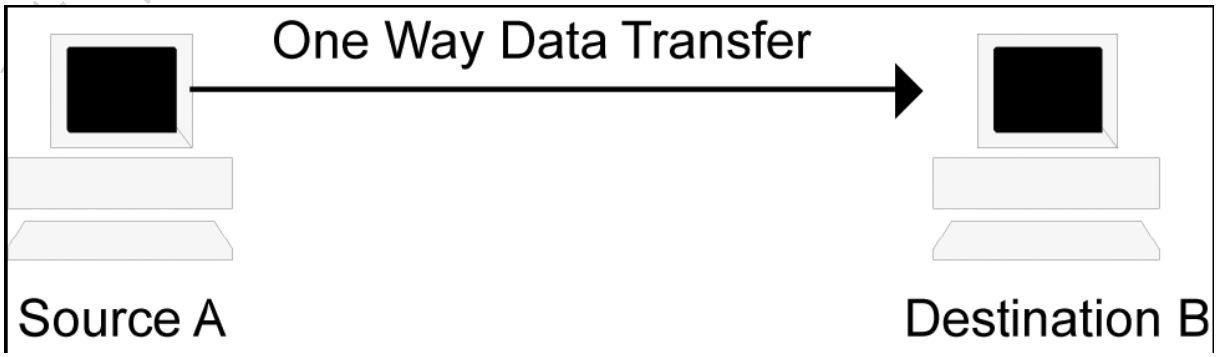
vi. Hybrid: In this, several topologies as subnetworks are linked together in a larger topology.



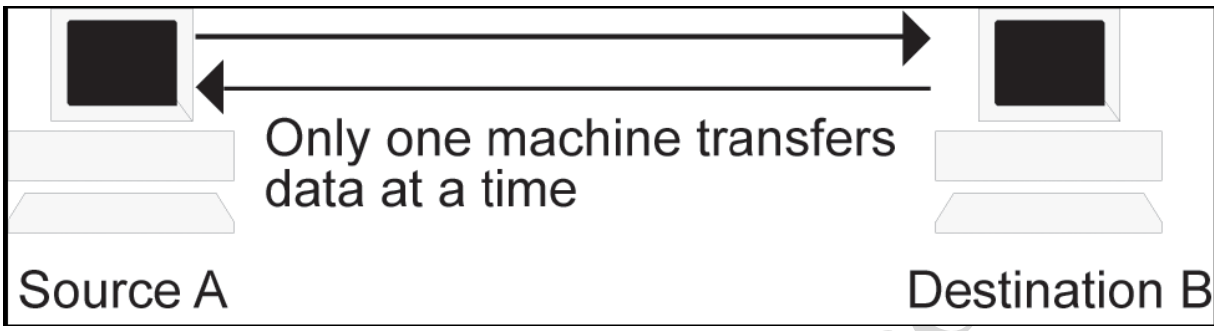
3. **TRANSMISSION MODE** (T.M.): The term T.M. is used to define the direction of signal flow between two linked devices. There are three types of T.M.:

(i) Simplex
(ii) Half Duplex
(iii) Full Duplex

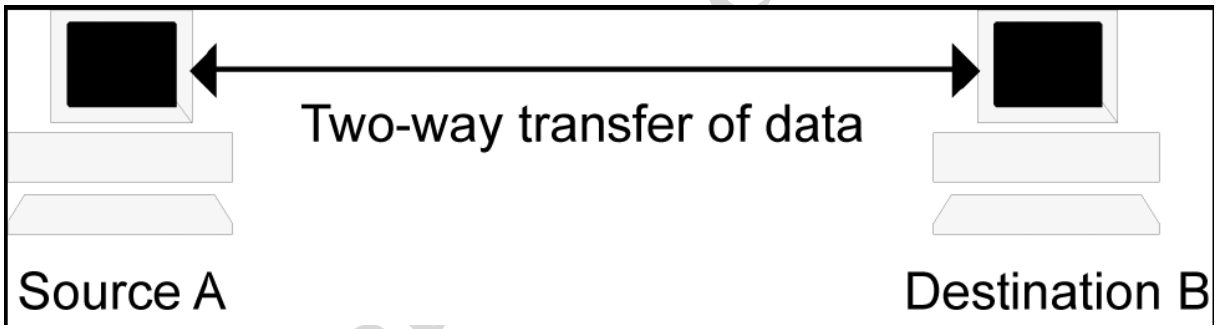
(i) Simplex: in simplex mode, the communication is unidirectional, like a one-way street, only one of the two stations can transmit, other can only receive. Keyboard and monitors are examples of simplex devices.



(ii) Half Duplex: In half duplex, each station can both transmit and receive, but not at the same time. When one device is sending data, the other can only receive and vice versa.



(iii) Full Duplex: In a full duplex mode, both stations can transmit and receive simultaneously. It is like a two-way street. The traffic can flow in both the directions at the same time.



4. **CATEGORIES OF NETWORKS**:

(i) LAN
(ii) MAN
(iii) WAN

(i) Local Area Network (LAN). It is a privately established network within a single building or campus of up to few Km in size. They are widely used to connect PC's and WS's within company offices and factories to share resources, for example printer, and to exchange information. It has three characteristics:

(a) Their size.
(b) Transmission technology.
(c) Their topology.

Single Building LAN:

a) They are restricted in size which means the worst case transmission time is bounded and known in advance.
b) LAN's may use a transmission technology consisting of cable to which all the machines are attached.
c) Various topologies are possible for LAN i.e. ring, star, bus etc.

(ii) Metropolitan Area Network (MAN): It is designed to extend over an entire city. It may be a single network such as a cable television network or it may be a means of connecting a number of LAN's into a larger network so that resources may be shared LAN to LAN as well as device to device. For example, a company may use a MAN to connect the LAN's in all of its offices throughout the city. A MAN may be completely operated by a private company or it may be a service provided by a public company such as a local telephone company.

(iii) Wide Area Network (WAN): WAN provides long distance transmission of data, voice, image and video information over large geographical areas (country or continent). It contains a collection of machines intended for running user programs. These machines are called hosts. These hosts are

connected by a communication subnet. The job of the subnet is to carry messages from host to host, just as telephone system carries words from speaker to listener. In most WAN's the subnet consists of two components:

(a) Transmission Lines: move the bits between machines. They can be made of copper wire, optical fiber or even radio links.

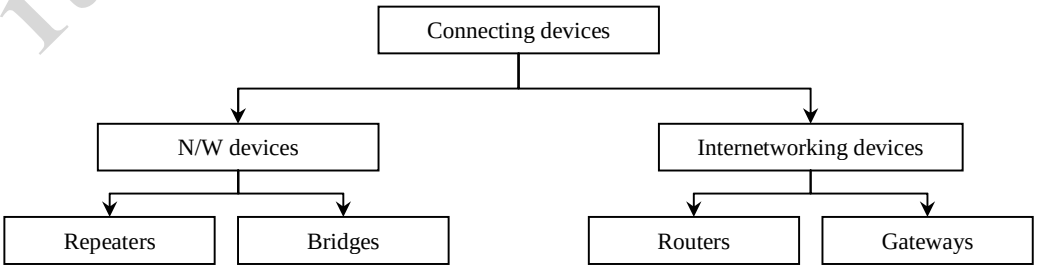
(b) Switching Elements: are specialized computers that connect three or more transmission lines. When data arrives on an incoming line, the switching element must choose an outgoing line.

In WAN, the network contains a number of transmission lines, each one connecting a pair or route.

5. **INTERNETWORK**: when two or more networks are connected they become an internetwork or internet. Individual networks are joined into internetwork by the use of internetworking devices. These devices are called routers and gateways.

LAN and WAN Devices

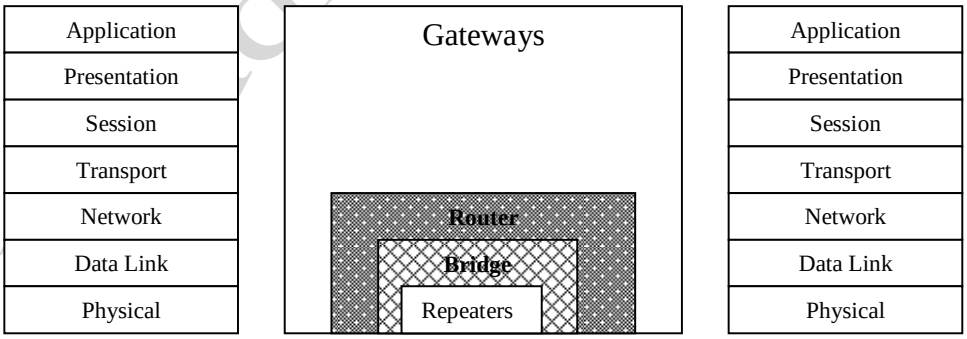
Network devices are divided into 4 categories:



Each of these devices interacts with protocol at different layers of the OSI model. In first case the device **Repeaters** or **Regenerators** is inserted into the N/W to increase the coverable distance. The other device bridge is inserted for traffic management.

When two or more separate network is connected for exchanging data or resources they become an ***inter-network (INTERNET).*** Linking a number of LAN's into an internet requires additional inter networking devices called **routers** and **gateways**.

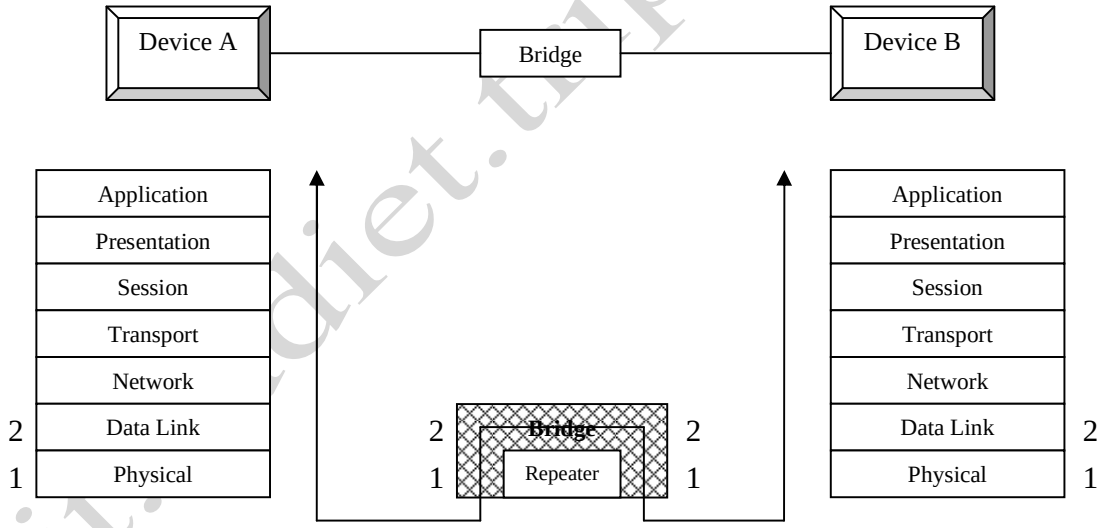
1) Repeaters act only upon the electrical components of a signal and there for active only at the physical layer.
2) Bridges utilize addressing protocols and can affect the flow control LAN; they are most active at the data link layer.
3) Routers provide links between two separate but same types LAN's and are most active at the network layer.
4) Gateways provide translation services between incompatible LANs or applications and are active in all of the layers.



BRIDGE

Bridges operate in both the physical data link layers of OSI model. Bridges can divide a large network into smaller segments. They can also relay frames between two separate LANs. The bridges contain logic that allows them to keep the traffic for each segment separate. So bridges can also provide security through this partitioning of traffic.

A bridge operates in data link layer giving it access to the physical address of all the stations connected to it. When a frame enters in a bridge, the bridge not only regenerates the signal but checks the address of the destination and forward the frame to the segment to which the address belongs. As bridge encounters a frame, it reads the address contained in the frame and compares that address with the table of all the stations on both segments. When it finds a match, it discovers to which segment the station belongs and forwards the frame.



BRIDGE IN OSI MODEL

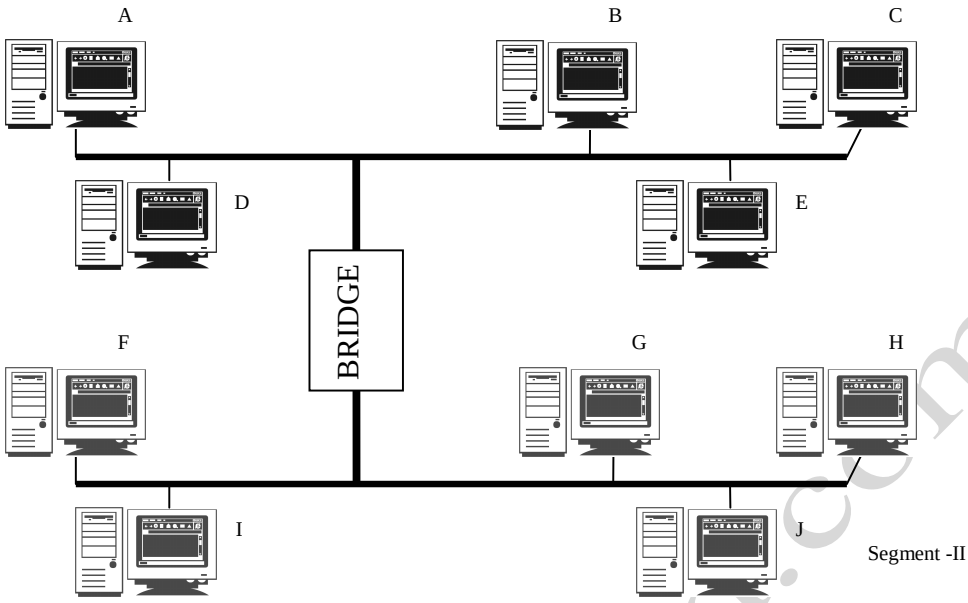


Figure shows a Bridge that is joining two segments.(segment I- upper segment, segment II – lower segment)

A packet from A to E is addressed. Packet arrives at the bridge. Both stations are at the same segment therefore the packet is blocked to go into the lower (II) segment.

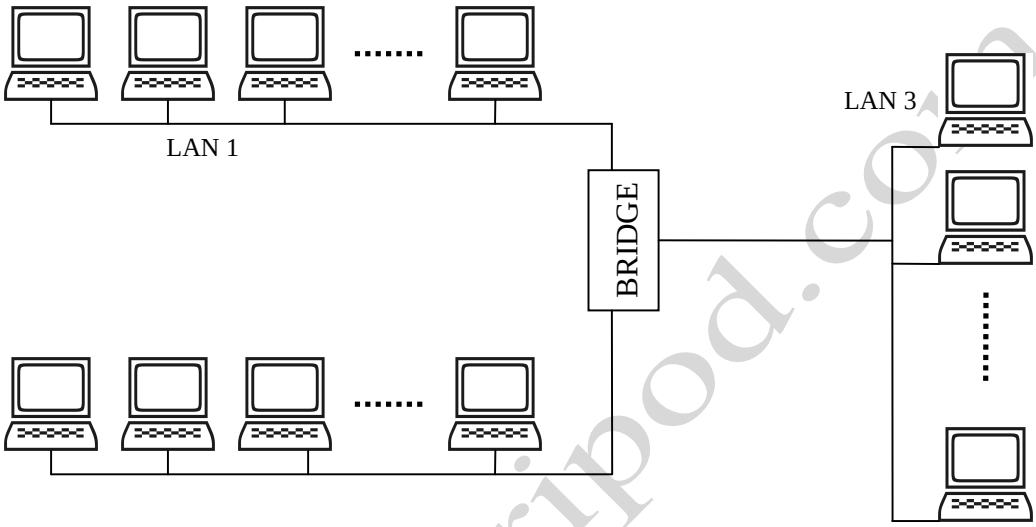
But if a packet wants to go from station A to station J then it arrives at the bridge. The bridge checks the destination station and allows it to enter into the lower segment where it is received by station J.

There are three types of bridges:

1) **Simple bridge:** these are most primitive and least expensive type of bridge. A simple bridge links two segments and contain a table that links the addresses of all the stations. Each address is entered manually. Before a simple bridge can be used an operator must sit down and enter the address

of every station. When a new station is added or deleted then the table must be modified manually.

2) **Multiport bridge:** a multiport bridge can be used to connect more than two LANs



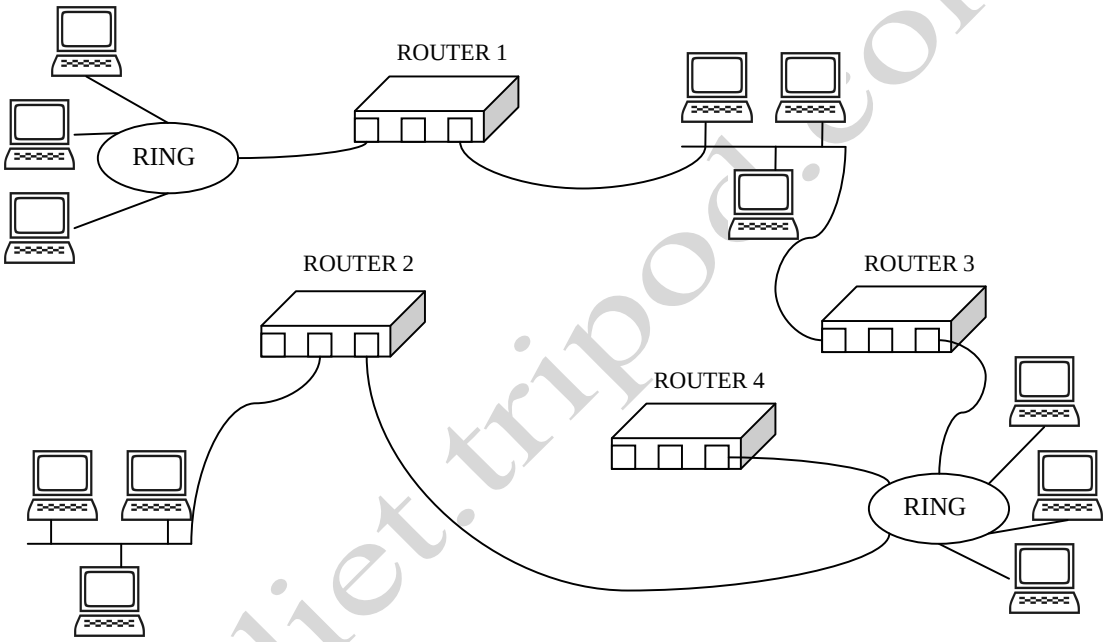
3) **Transparent bridge:** it builds its table of station addresses on its own as it performs its bridge function. When it is just installed its table is empty. As it encounters each packet it looks at both the destination and source address.

ROUTERS:

Routers operate at *network layer*. They connect two or more network segments that use the same or different data link protocols but the same network

protocol. They can access network layer addresses and contain software that enables them to determine which of the several possible paths between these addresses the best for a particular transmission is.

Routers relay packets among multiple interconnected networks. They route packets from one network to any no. of destination networks on an internet. Figure shows 5 network of a inter-network



A packet sent from a station on one network to a station on neighboring network goes first to the jointly held router which switches it over to the destination network.

So the major feature of a router is that it can choose the best route between the networks when there are several possible routes between them. They act like stations on a network. If there is no one router connected to both the sending and receiving networks, the sending router transfers the packet across

one of its connected networks to the router. That router forwards the packet to the next router on path and so on until the destination is reached.

For the best route the router uses the different routing algorithm.

REPEATERS:

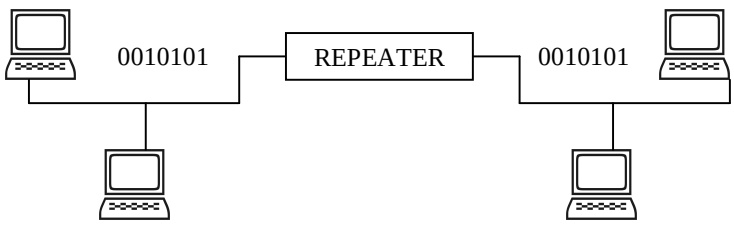
A repeater is also known as a regenerator. It is an electronic device that operates on only the physical layer of OSI model

It receives the incoming signal, translates it into a digital message and retransmits the message because the message is recreated at each repeater so noise and distortion from the previous circuit are not amplified. This provides a much cleaner signal and results in a lower error rate for digital circuit. Repeater is installed on a link. It receives the signal before it becomes too weak or corrupted, regenerates the original bit pattern and put the refreshed copy back onto the link

They do not understand frames, packets or headers. They understand volts.

A repeater allows us to extend only the physical length of a network.

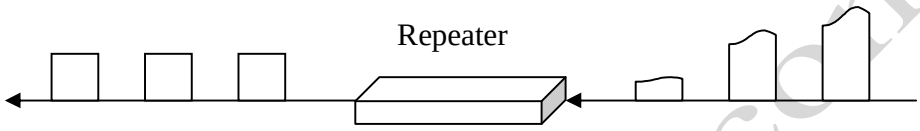
Figure shows the two sections connected by the repeater



Fugure A

Function of a repeater is also shown in figure B

Figure B



Regenerated signal Corrupted

Signal

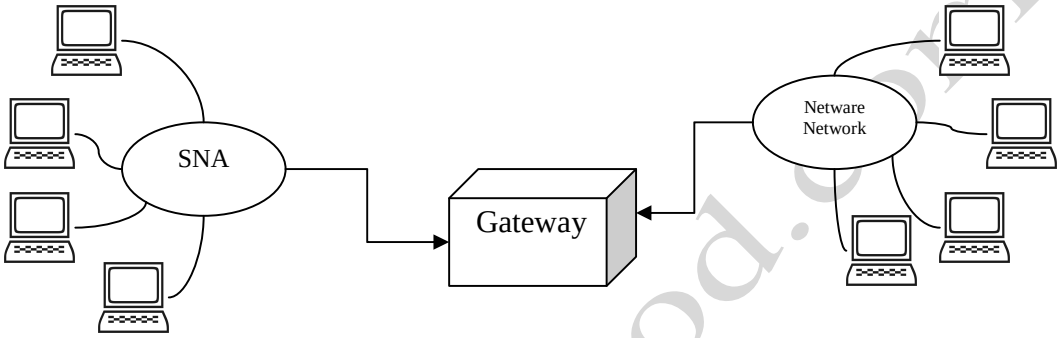
GATEWAYS

Gateways are more complex than bridges or routers because they are the *interface between two or more* ***dissimilar networks.*** Gateways process only those messages which are explicitly addressed to them and route those messages that need to go to other networks

Gateways translate one network layer protocol into another, translate data link layer protocols and open sessions between application programs. More complex gateways even take care of such task as code conversion (eg: converting from ASCII into EBCDIC). A gateway may be stand alone computer with several

networks and special software connected to a main frame computer. It is also used to adjust the data rate, size and format.

Figure shows a gateway connecting an SNA N/W (IBM) to a NETWARE N/W



Gateways provide both the basic system interconnection and necessary translation between protocols in both the directions.

HUB:

A hub has a no. of input lines that it joins electrically. Frame arriving on any of the lines are sent out on all the others. All lines coming into a hub must operate at the same speed as shown in fig (a)

Network hubs serve two purposes. First they provide an easy way to connect network cables. It is just like a junction box permitting new computers to be connected to the network as easily as plugging an electrical socket. Each connection point where a cable can be plugged is called a port. Each port has a unique number.

Simple hubs are commonly available in 4-,8-,16- and 24- port sizes when no cables are plugged in the signal by passes the unused port. When cable is plugged into a port, the signal travels down the cable as though it were directly connected to the cables attached to the hub. Some hubs also enable different types of cable to be connected and perform necessary conversions (eg: twisted pair wire to co-axial cable, co-axial cable to fiber optic cable)

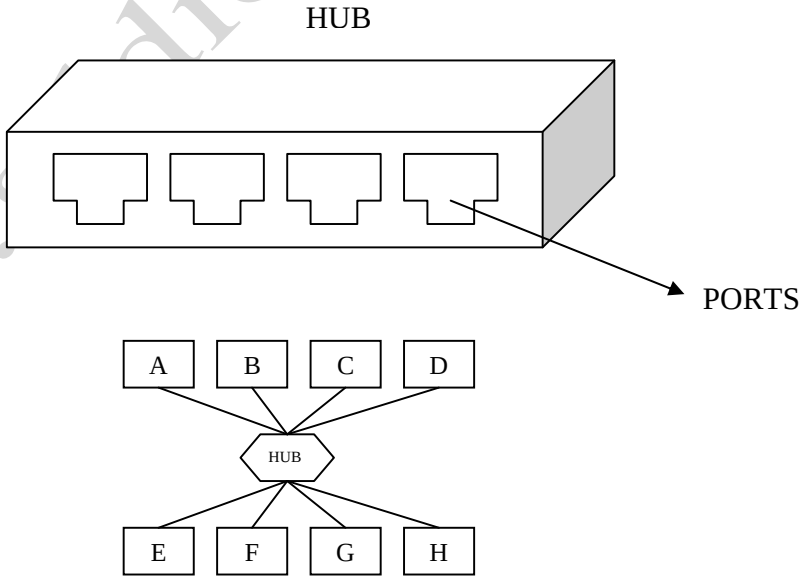


Fig (a) and (b)

Hub are of two types :

1. Active Hub
2. Passive Hub

MODEM:

Hardware circuits that accept a segment of data bits and apply modulation to a carrier wave according to the bits are called a ***modulator*****.**

A hardware that accepts a modulated carrier wave and recreates the segment of data bits that was used to modulate the carrier is called a ***demodulator*****.**

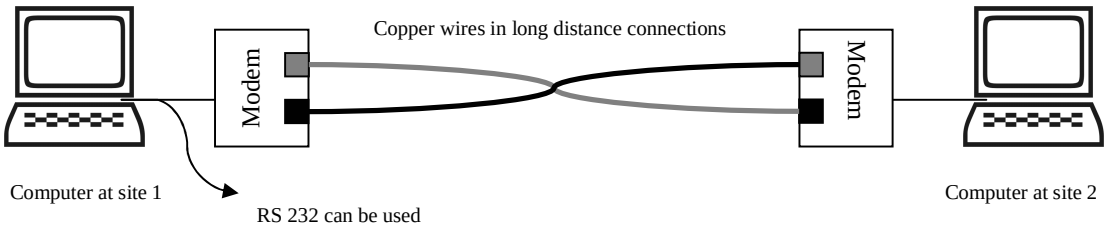
Thus, transmission of data across a long distance requires a modulator at one end and a demodulator at the other end.

Most network systems are full duplex. To support such full duplex communications each location needs both a modulator and a demodulator for transmitting and receiving the data respectively.

To keep the cost low and make the pair of devices easy to install and operate, manufacturers combine both circuits in a single device called ***modem***

Modem stands for modulator / demodulator

Figure shows how a pair of modems can be used to connect two computers across a long distance.



So each modem contains a separate circuitry to send and receive digital data.

The modems that coordinate sending data are called half-duplex or two-wire modem.

To coordinate the pair of two wire modems agrees to take turn. One modem sends the data and then allows the other modem to send data. This co-ordination occurs automatically. The user remains unaware that the modems are taking turns.

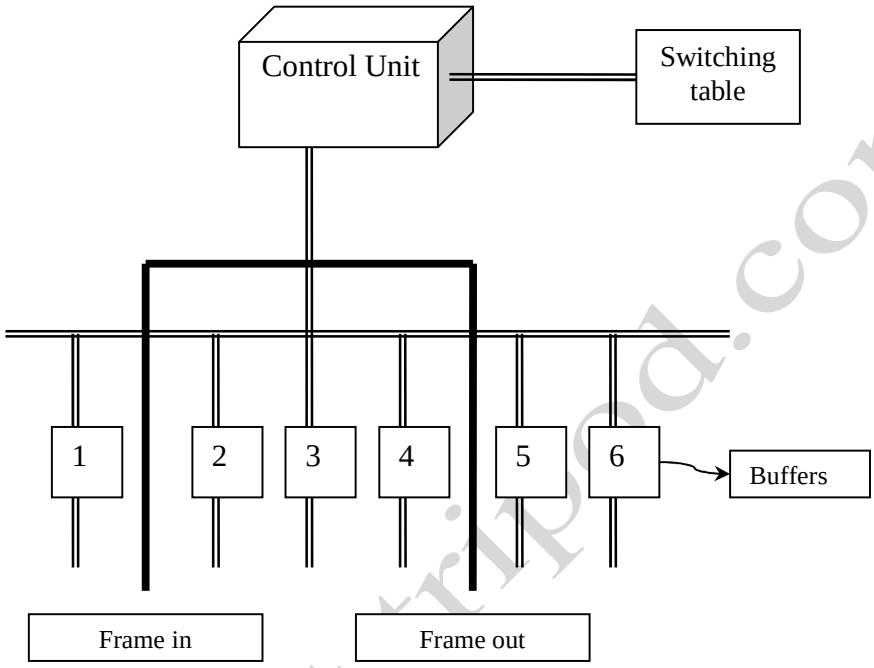
In addition to wires, modems are also used with other media RF transmission and glass fibers.

1) **RF modems** can send and receive information by modulating a radio frequency carrier. They are used in wireless network technologies.
2) **Optical modems** can be used to send data across a pair of glass fibers using light.
3) **Dial-up modems** use the dialup telephone network to communicate. Dial –up modems must be able to dial or answer a telephone call.

ETHERNET SWITCH:

A switch is a device that provides bridging functionality. It may act as a multipart bridge to connect devices or segments in a LAN. The switch normally has a buffer for each link (network) to which it is connected. When it receives a packet it stores the packet in the buffer f the receiving link and checks the address to find the

outgoing link. If the outgoing link is free means no chance of collision then the switch sends the frame to that particular link.



Switches are based on two different strategies

1) Store-and-forward

In this type, switch stores the frame in the input buffer until the complete packet has arrived.

2) cut-through

In this type of switch it forwards the packet to the output buffer as soon as the destination add is receive. Figure shows the concept of the switch

A frame arrives at part 2 and is stored in a buffer. The control unit checks the switching table to find the output port. The frame is then sent to port 5 for transmission.

A new generation of switches that are a combination of a router and a bridge has recently appeared. These "routing switches" use the network layer destination address to find the output link to which the packet should be forwarded. This process is faster than the use o simple switch.

ADDRESSING

In addition to the physical addresses, the internet requires an additional addressing convention: an address that identifies the connection of a host to its network. So the identifier used in the network layer of the internet model to identify each device connected to the internet is called the internet address or IP address.

Each internet address consists of four bytes (32 bits) defining three fields: class type, netid and hostid. These parts are of varying lengths, depending on the class of the address.

IP addresses are unique. They are unique in the sense that each address defines one and only one connection to the internet. Two devices on the internet can never have the same address at the same time. If a device has two connections to the internet via two networks, it has two IP addresses.

IP ADDRESSES ARE UNIQUE AND UNIVERSAL

CLASS TYPE	NETID	HOSTID

There are two common notations to show an IP address:

1. Binary Notation

2. Dotted Decimal Notation

1. BINARY NOTATION: In binary notation, an IP address is displayed as 32 bits. To make the address more readable, one or more spaces are inserted between each octet (8 bits). Each octet is often referred to as a byte. So, IP address is referred to as a 32-bit address, 4-octet address or a 4-byte address. The example of an IP address in binary notation is:

   01110101 10010101 00011101 11101010

2. DOTTED DECIMAL NOTATION: To make the IP address more compact and easier to read, IP addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Fig shows the IP address in dotted decimal notation. Because each byte is only 8-bits, each number in the dotted decimal notation is between 0 and 255.

   10000000 00001011 00000011 0001111

   128. 11. 3. 31

Example 1: Convert the following IP addresses from binary to decimal notation.

(i) 10000001 00001011 00001011 11101111

Ans. 129.11.11.239

(ii) 11111001 1001101 1111101 00001111

Ans. 249.155.251.15

Example 2: Convert from decimal notation to binary notation.

(i) 111.56.45.78

Ans. 01101111 00111000 00101101 01001110

(ii) 75.45.34.78

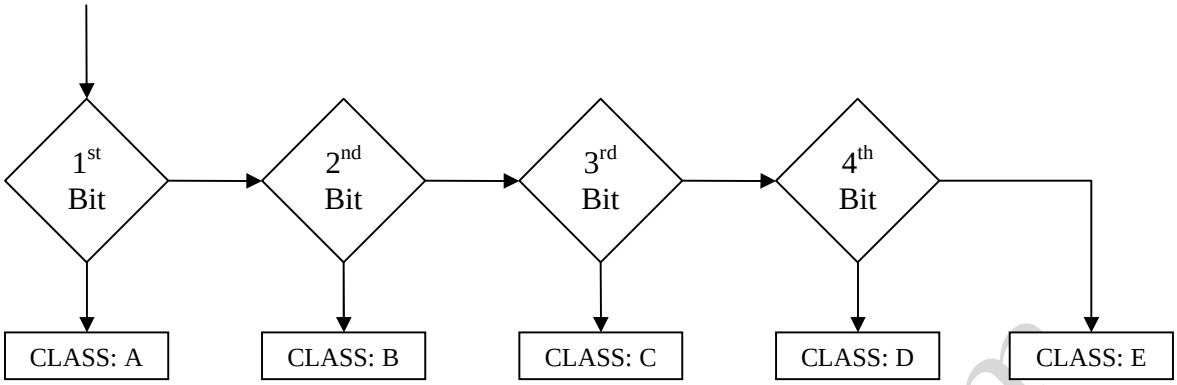
Ans. 01001011 0010101 00100010 01001110

CLASSFUL ADDRESSING: IP addresses use the concept of classes. This architecture is called classful addressing. In classful addressing the IP address space is divided into five classes: classes A, B, C, D and E. These classes are designed to cover different types of organizations.

Finding the Class in Binary Notation:

If the address is given in binary notation, the first few bits can immediately tell us the class of the address.

	Ist Byte	2nd Byte	3rd Byte	4th Byte
CLASS A	0			
CLASS B	10			
CLASS C	110			
CLASS D	1110			
CLASS E	1111			



Example: Find the classes:

(i) 11110101 10001111 11111100 11001111

Ans. Class E

(ii) 01111011 10001111 11111100 11001111

Ans. Class A

(iii) 11011101 10001111 11111100 1100111

Ans. Class C

Finding the Class in Dotted Decimal Notation:

When the address is given in dotted decimal notation, then we need to look only at the first byte (no.) to determine the class of the address. Each class has a specific range of numbers.

	Ist Byte	2nd Byte	3rd Byte	4th Byte
CLASS A	0 to 127			
CLASS B	128 to 191			

CLASS C	192 to 223			
CLASS D	224 to 239			
CLASS E	240 to 255			

This means that if the first byte (in decimal) is between 0 and 127 inclusive, the class is A. If the first byte is between 128 and 191 inclusive, the class is B.

Example: Find the classes.

(i) 134.11.78.56

Ans. Class B

(ii) 252.5.15.111

Ans. Class E

(iii) 227.12.14.87

Ans. Class D

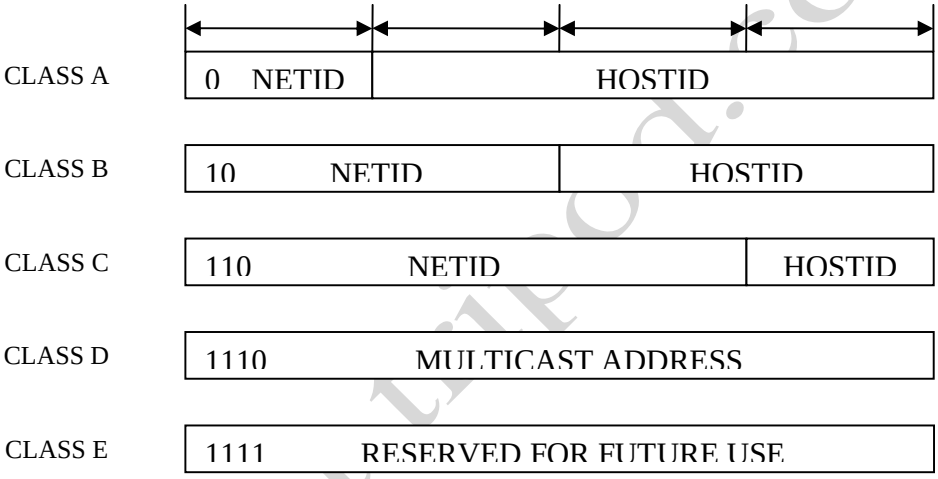
Addresses in class A, B and C are for unicast communication i.e. from one source to one destination. A host needs to have at least one unicast address to be able to send or receive packets.

Address in class D are for multicast i.e. communication from one source to a group of destinations.

Addresses in class E are reserved. They have been used only in a few cases.

NETID AND HOSTID: In classful addressing, an IP address in classes A, B and C is divided into netid and hostid. These packets are of varying lengths depending upon the class of the address. Fig shows that here the classes D and E are not divided into netid and hostid.

In Binary Notation:



In Decimal Notation:

	FROM	TO
CLASS A	0. 0. 0. 0	127. 255. 255. 255
CLASS B	128. 0. 0. 0	191. 255. 255. 255
CLASS C	192. 0. 0. 0	223. 255. 255. 255
CLASS D	224. 0. 0. 0	239. 255. 255. 255
CLASS E	240. 0. 0. 0	255. 255. 255. 255

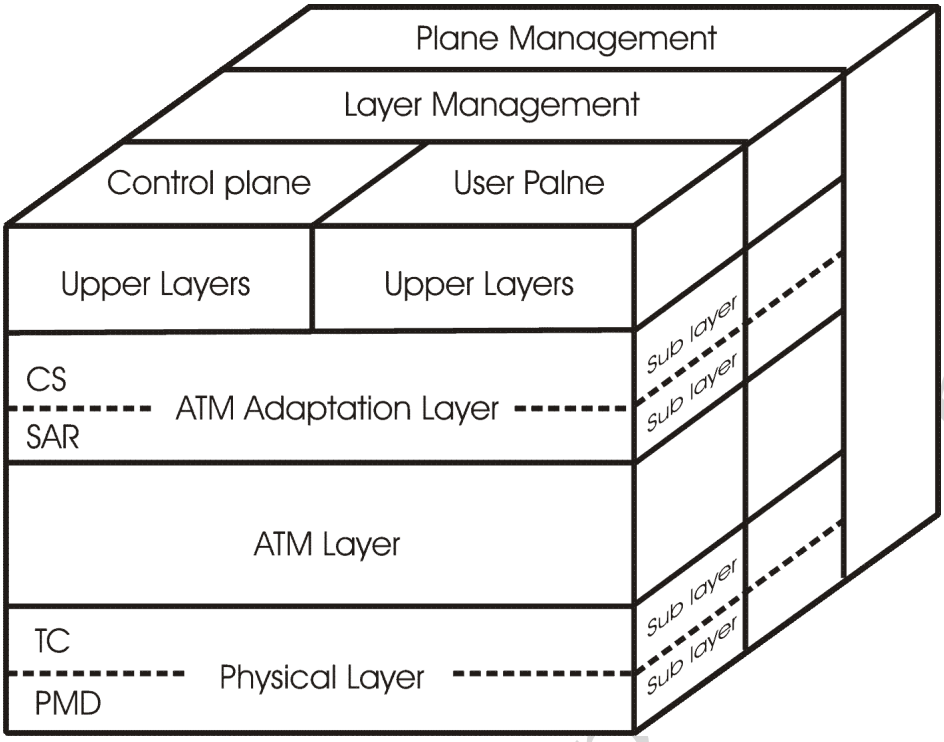
ATM and AAL LAYER PROTOCOL

ATM REFERENCE MODEL (ASYNCHRONOUS TRANSFER MODE)
(ATM is widely used within the telephone system)

ATM is a model that is different from the OSI model and also different from the TCP/IP. Figure shows the ATM model. It consists of three layers.

1) physical layer
2) ATM layer
3) AAL layer

Plus whatever users want to put on top of that.



CS- Convergence sub-layer
SAR- Segmentation and reassembly sub-layer
TC- Transmission convergence sub-layer
PMD-Physical medium dependent sub-layer

1) Physical layer:

It deals with the *physical medium, voltages, bit timing, bit synchronization* and other issues also. Physical layer is divided into two parts:

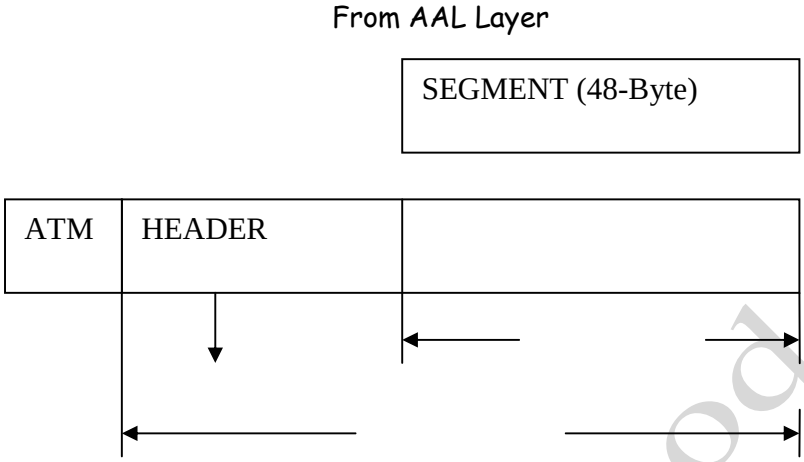
a) TC- transmission convergence sub-layer
b) PMD- physical medium dependent

i) **PMD:** this sub-layer interfaces with the actual cable. It moves the bit on and off. And handles the bit timing. For different carriers and cables this layer will be different.

ii) TC: this is the upper part of the physical layer. When cells are transmitted the TC layer sends them as a string of bits to the PMD layer. At the other end (destination) the TC sub-layer gets a incoming bit stream from the PMD sub-layer. Its job is to convert this bit stream into cell stream for the ATM layer. It handles all the issues related to telling where cells begin and end in the bit stream.

2) ATM layer:

It deals with cell and cell transport. It defines the layout of a cell and tells what the header fields mean. It also deals with establishment and release of VC congestion control is also located here.
It processes outgoing traffic by accepting 48-byte segments from the AAL layer and transform them into 53-byte cells by the addition of a 5-byte header.



HEADER FORMAT: ATM uses two formats for the header:

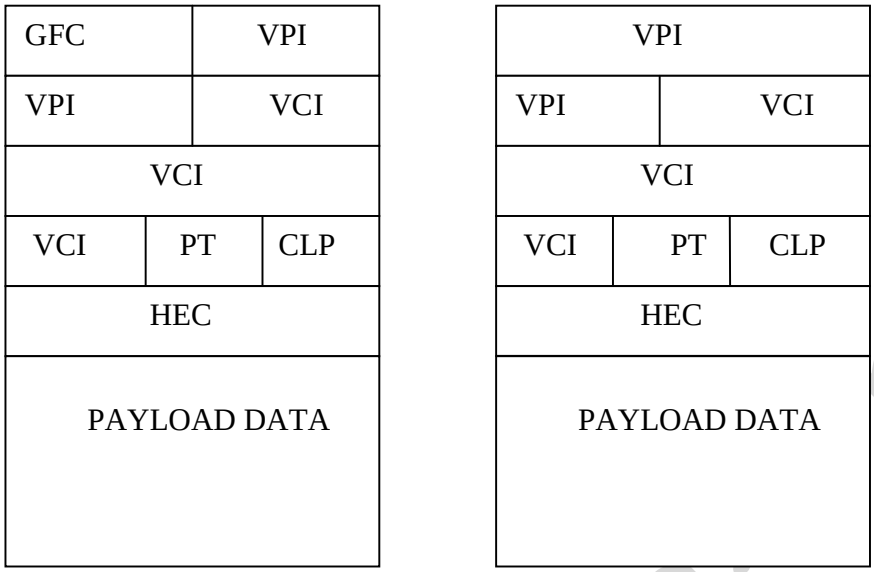
1) user to network interface(UNI)
2) network to network interface(NNI)

ATM headers:

HEC→ (header error correction): it is used to *detect and correct errors*. It is like CRC.

VCI→ (virtual channel identifier): it is a **16-bit** field in both cells. When VC is established then it is used as *an identifier for VC channel*.

VPI→ (virtual path identifier): it is an **8-bit** field in **UNI** and **12-bit** field in **NNI** cell and used as *an identifier for VC path*.



UNI Cell NNI cell

PT→ (payload type): it is a **3-bit** field. The first bit defines the payload as user data or managerial information. The last 2-bits depend on the first bit.

CLP→ (cell loss priority): it is **one-bit** field and used for *the congestion control.*

GFC→ (generic flow control): it is a **4-bit** field and ***present only in UNI cell***. It *provides flow control.*

3) AAL layer:
This layer is divided into two parts as shown in figure.
The upper part is called **CS (convergence sub-layer)** and the lower part is called **SAR (segmentation and reassembly sub-layer)**

SAR→ the SAR breakup the packets into cells on transmission side and puts them back together again at the destination side.
It also adds headers and trailers to the data unit. Then these payloads are then given to the ATM layer for transmission.

CS→ this sub-layer is concerned with the messages. Its job is to provide the interface to the application.

AAL TYPES

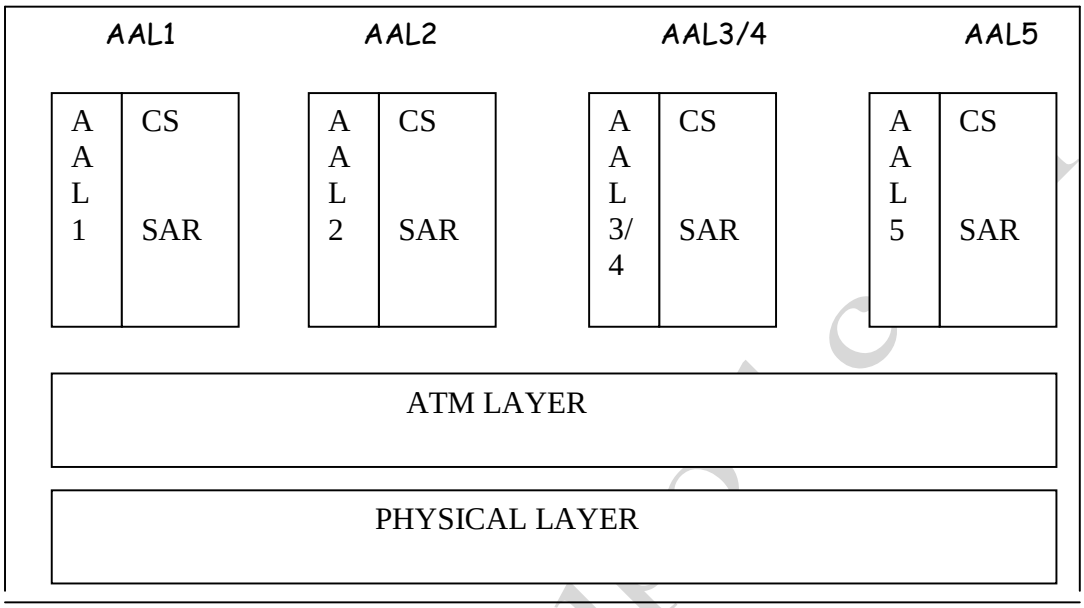


FIGURE (b)

As shown in figure (b) ATM defines for versions of the AAL:

1) AAL1
2) AAL2
3) AAL3/4
4) AAL5

These versions are divided because of 3 different reasons.

1) Real time service versus non real time-service.
2) Constant bit rate versus variable bit rate
3) Connection oriented service versus connection less service

AAL1:

It supports applications that transfer the information at constant bit rates in real time. It uses the connection oriented service, such as uncompressed audio and video.

In AAL1 the CS divides the bit stream into 47 byte segments and passes them to SAR sub-layer. Then SAR accepts 47-byte payload from the CS and adds one byte header. The result is 48-byte data unit. It is then passed to the ATM layer where it is encapsulated in a cell.

AAL1	CS	47-byte
	SAR	
ATM		

SN→ (Seq. no): it is a ***4-bit field*** that defines ***the sequential no. to order the bits***. The first bit is sometimes used for timing which leaves 3-bits for sequencing.

SNP→ (Seq. no. protection): the second field is also ***4-bit***. It protects the first field. The ***first 3-bits*** automatically ***correct the SN field***. The ***last bit*** is used as a ***parity bit***. In this parity bit detects an odd no. of errors but not an even no. of errors.

AAL2:

AAL2 was originally intended to support a variable data rate bit stream, but it has been redesigned. It is ***now*** used for ***low-bit rate traffic*** and ***short frame traffic*** such as audio, video or . A good example of AAL2 use is in mobile telephony. AAL2 allows the ***multiplexing of short frames into one cell***.
The SAR cell format is shown in figure. It has a ***one-byte header*** and ***2-byte trailer*** and ***data unit*** is of ***45-byte***.

SN Field→ (Seq. no): it is used for numbering cell in order to detect missing or mis-inserted cells. It is a **4-bit** field.

IT Field → (information type): it is also **4-bit** field. It is used to indicate that the cell is at the start, in middle or at the end of a message.

LI→ (Length indicator): this field tells how big the payload is in bytes (it may be less than 45 bytes). It is a **6-bit** field.

CRC→ CRC field is checksum over the entire cell, so by this the errors can be detected. It is a **10-bit** field.

AAL3/4:

Initially **AAL3** was intended to support ***connection-oriented*** data services and **AAL4** to support ***connectionless*** service. The fundamental issues of the two protocols were the same. So they are combined into a single format called AAL3/4. AAL3/4 can operate in two modes:

1) stream mode
2) message mode

In ***message mode*** each call from the application to AAL3/4 injects one message into the network. The message is delivered as such, message ***boundaries are preserved***.

In ***stream mode*** the boundaries are ***not preserved***.

In AAL3/4 the message of 65, 535 bytes come into convergence sub-layer from the application. These are just padded out to a multiple of 4-bytes. Then a header and a trailer are attached as shown in figure.

CPI	B tag	BA size	Payload (1-65535 bytes)	Padding		E tag	Length

CS header CS trailer

CPI (COMMON PORT INDICATOR)

It gives the message type and counting unit for BA size and length fields. This is an ***8-bit*** field.

B tag and E tag (ending tag)

These fields are used to frame the messages. The two bytes must be the same and are incremented by one on every new message sent. This mechanism checks for lost or mis-inserted cells. This is also ***8-bit*** field.

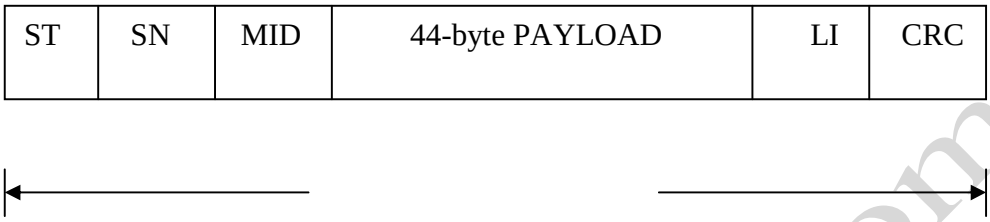
BA size (BUFFER ALLOCATION SIZE)

This is ***16-bit*** or ***2-byte*** field. This is used for buffer allocation. It tells the receiver how much buffer space to allocate for the message.

(CS TRAILER TERMS)

LENGTH (L)

The length field gives the payload length again. In message mode, it must be equal to BA size but in stream mode it may be different.
The trailer also contains 1 unused byte. After the convergence sub-layer has constructed and added a header and trailer to the message and passes it tot the SAR sub-layer. The cell format is shown in figure



ST (SEGMENT FIELD): it is used for message framing. It indicates whether the cell begins a message, is in the middle of a message is in the last cell of a message. It is a ***2-bit*** field.

SN (seq. no.): it is a ***4-bit*** field. It is used for detecting missing and mis-inserted cells.

MID (MULTIPLEXING IDENTIFICATION): this field is used to keep track of which cell belongs to which session. This is ***10-bit*** field that identifies cells coming from different data flows and multiplexed on the same virtual connection.

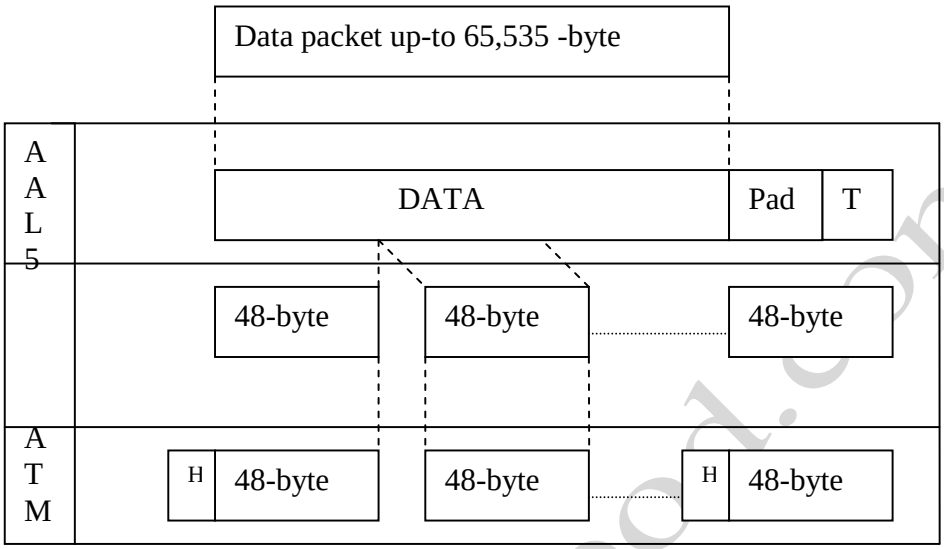
LI (LENGTH INDICATOR): the ***6-bit*** LI field indicates how much of the final packet data is.

CRC: this is a ***10-bit*** field. This is used to detect the errors.

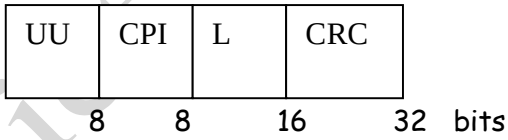
Note: the main feature of AAL3/4 is multiplexing.

AAL5:
AAl3/4 provides comprehensive sequencing and error control mechanisms that are not necessary for every application. For these applications the designers of ATM have provided a fifth AAL sub-layer called ***SEAL (SIMPLE EFFICIENT ADAPTION SUB-LAYER)*** AAL assumes that all cells belonging to a single message travel sequentially and that control functions are included in the upper layers of the ending application. In AAL5 the header field is not added in CS. Only padding and a four field trailer are added at the CS. So, it does not contain addressing, seq. or other header information.
So CS accepts a data packet of no more than 65, 535 byte from an upper layer service and adds an 8-byte trailer as was required by padding field.

After that the CS passes the message in 48-byte segments to the SAR layer. It supports both message mode and stream mode.



CS trailer include



As shown in figure in AAL5 CS has only trailer field not the header field.

UU (USER TO USER)
The field is used by end users. It is available for a higher layer for its own purpose. For example: Seq. or multiplexing. It is an ***8-bit (1-byte)*** field.

LENGTH
It is a ***2-bit*** field. It tells how long the true payload is in bytes not counting the padding.

CRC
This is a ***32-bit*** field and used for error control on entire data unit.

In AAL5 this message is transmitted by passing it to the SAR sub-layer which does not add any headers or trailers. Instead it breaks the message into 48-byte units and passes each of them to the ATM layer for transmission.
The **main advantage** of AAL5 over AAL3/4 is **much greater efficiency** while AAl3/4 adds only 4-byte per message. It also adds 4-byte per cell reducing the payload capacity to 44-bytes, a loss of 8% on long message.
AAL5 has a large trailer per message but has no overhead in each cell. Long CRC (32-bit) field is used to detect lost, mis-inserted or missing cells without using Seq. no.

IPV6 (Internet Protocol Version 6)

The new version of IP is IP Version 6. It is also known as IPng (IP next generation). Some of the Changes from IPV4 to IPV6 include:

1. **Longer address field:** The length of address field is extended from 32 bits to 128 bits. The address structure also provides more levels of hierarchy.
2. **Simplified Header format:** The header format of IPV6 is simpler than that of IPV4 header. Some of the header fields in IPV4 such as checksum, IHL, Identification, Flags & fragment offset do not appear in the IPV6 header.
3. **Flexible support for options:** The options in IPV6 appear in optional extension headers that are encoded in more efficient & flexible way as compare to IPV4.
4. **Security:** IPV6 supports built in authentication & confidentiality.
5. **Large packet:** IPV6 supports payloads that are larger than 64Kb is called jumbo payloads.
6. **Flow label capacity:** IPV6 adds a 'flow label' to identify a certain packet flow that requires a certain QoS.
7. **No checksum field:** The checksum field In IPV6 has been removed to reduce packet processing time in a router.

Header Format:

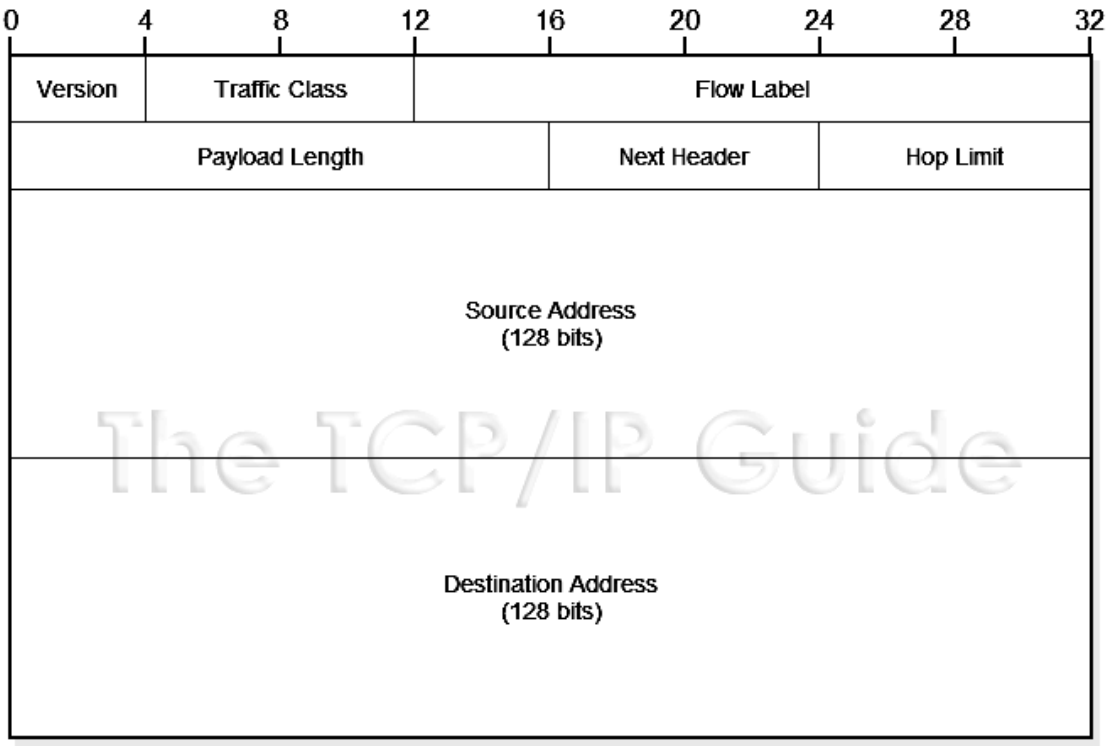


Fig (i) IPV6 Basic Header

The IPV6 header consists of required basic header optional extension headers. Fig (i) show the basic header format. The description of each field is as follows:

1. **Version**: The version field specifies the version no of the protocol & should be set to 6 for IPV6 (Bin Value 0110)
2. **Traffic Class**: The traffic class field specifies the traffic class or priority of the packet.
3. **Flow label**: A flow label is defined as a sequence of packets sent from a particular destination. The flow label can be used to identify the QoS request by the packet.
4. **Payload length:** The payload length indicates the length of data (excluding header) it is a 16 bit field so the payload is limited to 65,535 bytes
5. **Next Header:** The next header field identifies the type of the extension header that follows the basic header. The extension header is similar to the options field in IPV4, but is more flexible & efficient.
6. **Hop Limit:** The hop limit field replaces the TTL (Time To Live) field in IPV4. The value of this field specifies the number of hops the packet can travel before being discarded by a router.
7. **Source Address & Destination Address:** The source address & destination address (128 bits) identifies the Source host & the Destination host respectively.

N/w Addressing

The IPV6 address is 128 bits long these addresses are divided into 3 categories:

i. Unicast: Addresses identify a single N/w interface.
ii. Multicast: Addresses identifies a group of N/w interfaces, typically at different locations. A Packet will be sent to all N/w interfaces in a group.
iii. Anycast: Addresses also identifies a group of N/w interfaces. A packet will be sent to only one N/w interface in a group, usually the nearest one.

IPV4 address typically uses the dotted decimal notation when communicated by people. But IPV6 use a hexadecimal digit for every 4 bits & to separate every 16 bits with a colon. An example is

4BF5 : AA12 : 0216 : FEBC : BA5F : 039A : BE9A : 2176

If the address is
4BF5 : 0000 : 0000 : 0000 : 000A : BE9A : 2176 : FEBC

It can be shortened to:
4BF5 : 0 : 0 : 0 : A : BE9A : 2176 : FEBC

Further shortening is possible where consecutive zero value fields appear. These fields can be shortened to with the double colon notation (::). The double colon notation can appear only once in an Address the address can be written as:

4BF5 : 0000 : 0000 : 0000 : BA5F : 039A : 000A : 2176
1st 4BF5 : 0 : 0 : 0 : BA5F : 39A : A : 2176
2nd 4BF5 :: BA5F : 39A : A : 2176

The dotted decimal notation of IPV4 can be mixed with the new hexadecimal notation
Ex: ::FFFF:128.155.12.198

IPV6 assign a few addresses for special purposes;

1. The address 0:: is called the unspecified address & is never used as a destination address.
2. The Address ::1 is used for a loop-back whose purpose is same as the loop-back address in IPV4
3. Another set of special addresses is needed during transition period where an IPV6 packet needs to be tunneled across an IPV4 N/w. These addresses, called IPV4 Compatible address, they are used by routers & host that are directly connected to an IPV4 N/w.

Extension Header:

To support extra functionalities that are not provided by the basic header, IPV6 allows an arbitrary number of extension headers to be placed between the basic header & payload. Extension headers act like options in IPV4. The extension headers are daisy chained by the next header field, which appears in the basic header as well as in each extension header Fig shows the use of next header field The extension headers must be processed in the order in which they appear in the packet. Six extension headers have been defined. They are listed in table.

Basic Header Next Header = TCP	TCP Segment

Basic header Next Header = Routing	Routing Header Next Header = Fragment	Fragment Header Next Header = TCP	TCP SEGMENT

Daisy Chain Extension Header

Header code	Header Type
0	Hop by Hop options Header
43	Routing Header
44	Fragment Header
51	Authentication Header
52	Encapsulating security payload Header
60	Destination Options Header

OSI

The Seven Layers Model

7) **Application** : Provides different services to the applications

6) **Presentation** : Converts the information

5) **Session** : Handles problems which are not communication issues

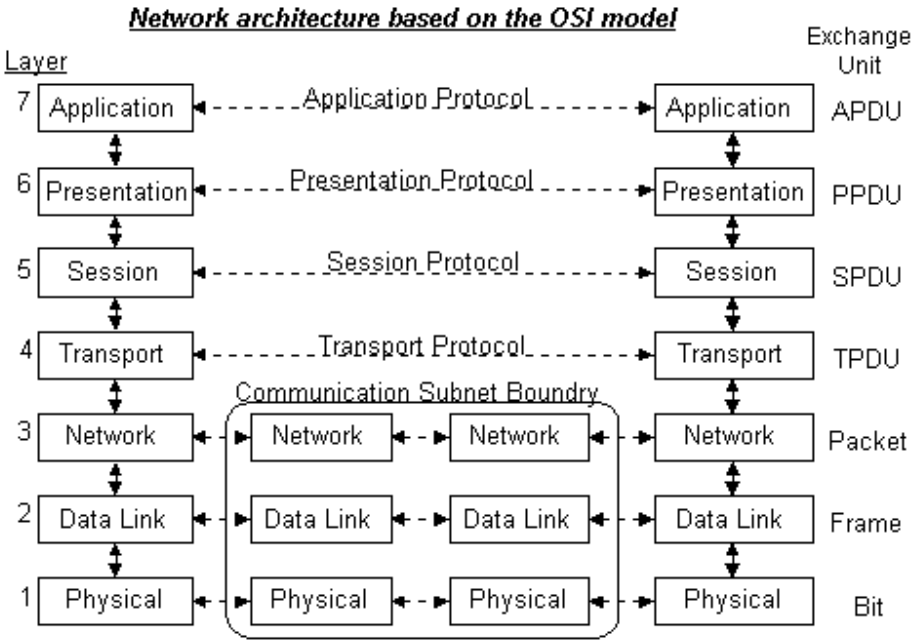
4) **Transport** : Provides end to end communication control

3) **Network** : Routes the information in the network

2) **Data Link** : Provides error control between adjacent nodes

1) **Physical** : Connects the entity to the transmission media

Please **D**o **N**ot **T**ouch **S**teve's **P**et **A**lligator
Physical **D**ata **L**ink **N**/w **T**ransport **S**ession **P**resentation **A**pplication



1. **Physical Layer**: the physical layer is concerned wit transmitting raw bits over a communication channel. It deals with mechanical & electrical specifications of the interface & transmission medium.

   Functions:

   (i) Representation of Bits: 0 & 1 into electrical or optical

   (ii) Data Rate (duration of bits)

   (iii) Synchronization of Bits: Sender and receiver must be clocked simultaneously.

(iv) Transmission Mode: Defines the direction of transmission between two devices i.e. simplex, half duplex or full duplex.

(v) It also deals with the physical characteristics of interfaces and media.

2. **Data Link Layer**: the main task of data link layer is to take a raw transmission facility and transform it into a line.

Functions:

(i) Framing: It divides the stream of bits into manageable data units called frames, transmit the frames sequentially and process the acknowledgement frames sent back by the receiver, make frame boundaries by attaching special bit pattern.

(ii) Physical Addressing: If frames are to be distributed to different systems on the network, the DLL adds a header to the frame to define the physical address of the sender as well as the receiver.

(iii) Flow Control: If the rate at which the data are absorbed by the receiver is less than the rate produced by the sender, then the data link layer makes a flow control. Some traffic regulation mechanism must be used.

(iv) Error Control: If due to noise or any other reason a frame is completely destroyed, the DLL has a mechanism to prevent duplication of frames.

3. **Network Layer**: The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks.

Functions:

(i) Logical Addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination system. The network layer adds a header to the packet coming from upper layer which includes the logical address of the sender and receiver.

(ii) Routing: Another main function of network layer is how the packets are routed from source to destination. The connecting devices called routers are used to route the packets to their final destination.

(iii) Congestion Control: If too many packets are present in the sub network at the same time, they form bottlenecks. The congestion control is done by network layer.

4. **Transport Layer**: Transport layer is responsible for source to destination delivery of the entire message.

Functions:

(i) Segmentation & Reassembly: A message is divided into transmittable segments, each segment containing a segment number. These numbers enable the transport layer to reassemble the message correctly upon receiving at the destination. It also identifies and replaces the packets that were last in the transmission.

(ii) Flow Control: Flow control between sender and receiver.

(iii) Error Control: It also deals with error control mechanism. Error control at this layer is performed end to end rather than across a single link.

5. **Session Layer**: It is the 5th layer. It is the network dialog controller. It establishes, maintains & synchronizes the inter-connection between communicating systems.

Functions:

(i) Dialog Control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place either in half duplex or full duplex mode.

(ii) Token Management: Another way of is token management. For some protocols it is essential that both sides do not attempt the same operation at the same time. To manage these activities the session layer provides tokens that can be exchanged. Only the side holding the token may perform the critical operation.

(iii) Synchronization: The session layer allows to add check points (synchronization point) into a stream of data.

6. **Presentation Layer**: Is concerned with the syntax and semantics of the information exchanged between two systems.

   Functions:

   (i) Translation: The processes in two systems are usually exchanging information in the form of character strings, numbers & so on. The information should be changed to bit stream before being transmitted because different encoding system. The P.L. at sender changes the information from its sender dependent format into a common format. The P.L. at the receiving machine changes the common format into its receiver dependent format.

   (ii) Compression: Data compression reduces the number of bits to be transmitted. It is useful in transmission of multimedia such as text, audio and video.

ENCRYPTION:

To carry sensitive information, a system must be able to assure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Application Layer: A.L. provides user interfaces and support for services such as email, file access & transfer (FAT), shared database management and other types of distributed information services.

Function:

(i) Mail Service: The A.L. provides the basis for email forwarding and storage.

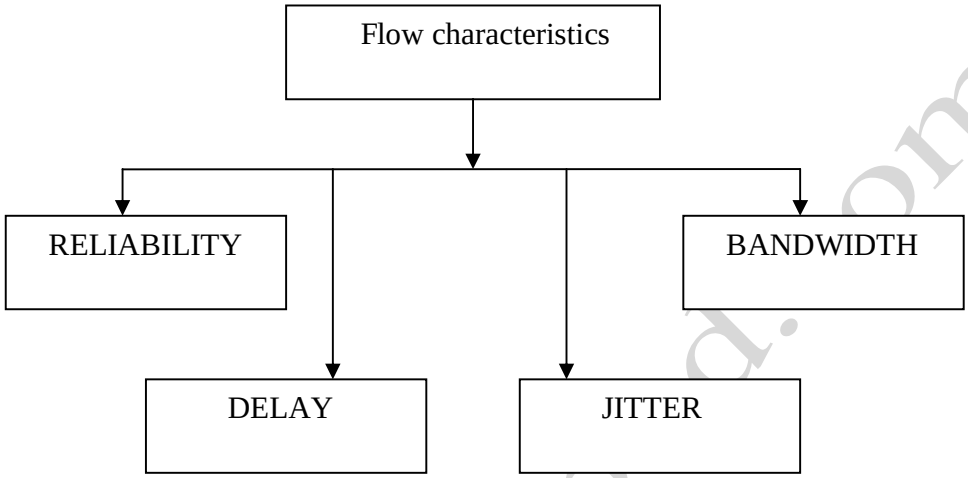
(ii) FTAM (file transfer and access management): The application allows a user to access file in a remote computer, to retrieve files in a remote computer.

Network Virtual Terminal: A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so the A.L. creates a software simulation of a terminal at a remote host. The user's computer talks to the software terminal, which in turn talks to the host and vice versa.

QOS (QUALITY OF SERVICE)

QOS is an internetworking issue that is defined as something a flow seeks to attain.

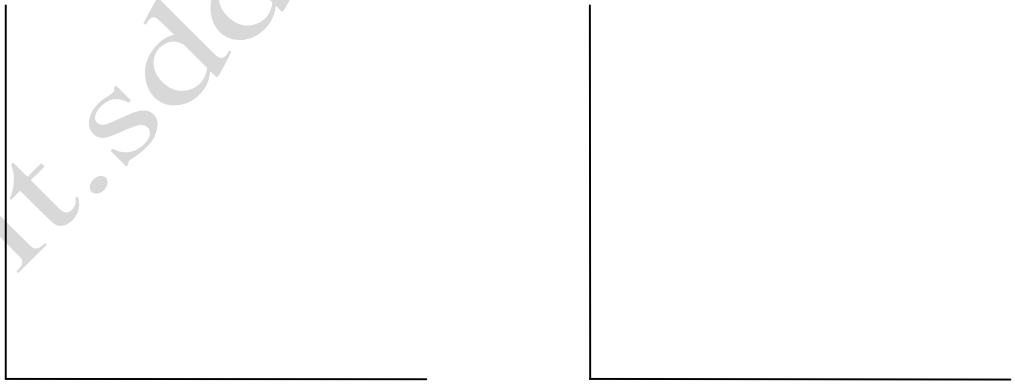
Flow characteristics:



JITTER:

Jitter is the variation in delay for packets belonging to the same flow. A network with jitter takes exactly the same amount of time to transfer each packet, while a network with high jitter takes much longer to deliver packets than others. Jitter is important when sending audio or video, which must arrive at regular intervals.

Jitter is illustrated in fig:



The jitter can be bounded by computing the expected transit time for each help along the path. When a packet arrives at a router, the router checks to see how much the packet is behind or ahead of its schedule. This information is stored in

the packet and updated at each hop. If the packet is ahead of schedule, it is held just long enough to get it back on schedule. If it is behind schedule the router tries to get it out the door quickly.

In this way, the packets that are ahead of schedule get slowed down and packets that are behind schedule get speedup, in both cases reducing the amount of jitter.

TTL ENCODING (TIME-TO-LIVE ENCODING)

TTL I an 8 bit field in the label stack that is used to encode a time to live value. In IP networks TTL is used to prevent packets to travel indefinitely in the network.

RULES:

TTL is decremented at each router-hop
If TTL=0 packet is discarded
TTL is present in the label header for PPP and LAN headers

Each label stack entry is broken down into the following fields:

1) BOTTOM OF STACK (S):
This bit is set to 1 for the last entry in the label stack and zero for all other label stack entries.

2) TIME TO LIVE (TT^2):
This 8-bit field is used to encode a time to live value.

3) EXPERIMENTAL USE(Exp):
This 3-bit field is reserved for experimental use.

4) LABEL VALUE (Label):
This bit is used for label value.

Label	Exp	S	TTL

The ***"incoming TTL"*** of a labeled packet is defined to be the value of the TTL field of the top label stack entry when the packet is received.

The ***"outgoing TTL"*** of a labeled packet is defined to be larger of

a) one less than the incoming TTL
b) zero

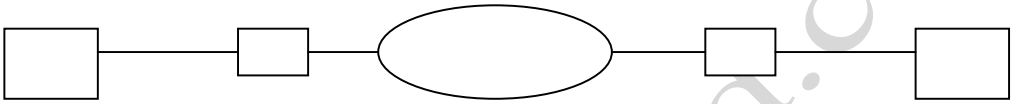
If the outgoing TTL of a labeled packet is zero then the labeled packet must not be stripped off and the packet forwarded as an unlabeled packet. The packet's life time in the network is considered to have expired.

Depending on the label value in the label stack entry, the packet may be simply discarded or it may be passed to the appropriate network layer for further processing.

When a labeled packet is forwarded, the TTL field of the label stack entry at the top of the label stack must be set to the outgoing TTL value.

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

To use a leased digital circuit one must agree to follow the rules of the telephone system. It may seem that following standards for digitized information would be trivial because computers are digital as well. Because, the computer industry and the telephone industry developed independently the standards, for telephone system digital circuit differ from those used in computer industry. Thus a special piece of hardware is needed to interface a computer to a digital circuit provided by a telephone company, known as **CSU/DSU**.
This device contains two functional ports usually combined into a single chassis.



A CSU/DSU is required at each end of leased circuit as shown in figure.

The **"CSU"** portion of the DSU/CSU device ***handles the termination and diagnostics***. For example, the CSU contains circuitry to accommodate current surges that are generated by lightning or other electromagnetic interference. It also contains ***diagnostic circuitry*** that can ***test whether*** the ***DSU/CSU on the other end is functioning correctly***. Finally, the CSU ***provides a loop back capability used when installing and testing circuits***. When loop-back is enabled, the CSU ends back copy of all data that arrives across the circuit without passing it through.
The **"DSU"** portion of the DSU/CSU ***handles the data***. It ***translates data between*** the ***digital format used on the carrier's circuit and the digital format required by the customer's computer equipment***. The interface standard used on the computer side depends on the rate that the circuit operates. If the data rate is less than 56 kbps, the computer can use RS-232. For rates above 56 kbps the computer must use interface hardware that support higher speeds.

LATENCY

Integrated applications (such as audio and video) rely on a consistent rate of delivery over a network so that movement and voice response are synchronized and do not have jerky or uneven playback. ***The time it takes to send information from the transmitting device to the receiving device is called "LATENCY".***

The goal on a well designed network for integrated multimedia applications is to have a minimum latency period and minimum variation in latency. For example, telecommunications based WAN's are designed to keep latency to less than 400ms. Most LAN's are designed to match the same latency.
Latency on a network is influenced by the following factors:

1) Transmission delay: is the time in which a packet travels across a network medium such as 10 BASE T cabling or 100 BASE-TX cabling. Besides the speed of the medium, transmission delay is influenced by the size of the packet.

2) Propagation delay: is the time it takes for a packet to travel a segment or network, end to end. Propagation delay is usually associated with fiber-optic media and the speed of light through the media.

3) Processing delay: is the time it takes for a bridge, switch or router to compare frame or packet contents with its table information, change the frame or packet header and avoids any special services such as packet translation and re-encapsulation or incrementing the hop count.

4) Store and forward or switching delay: is a time used by a bridge, switch or router to examine process and retransmit a frame or packet.

DISPERSION

The spreading, separation or scattering of a waveform during transmission

The related terms or types are:

1) chromatic dispersion
2) polarized modal dispersion

Chromatic dispersion: different wavelengths of light travel at different speed through a medium example: fiber optic cables. ***Chromatic dispersion is the measure of the relative velocity of light in adjacent wavelengths in the fiber***. The simplest demonstration of this is a prism. When you shine a light into a prism, the light that is emitted is broken out into the different frequencies or colors.

The impact of chromatic dispersions is that some light waves will arrive before other at the receiving end. If the light pulses arrive with too great a variance, the transmission will not be successful.

Polarized modal dispersion: Polarized modal dispersion is ***the distortion that occurs in the fiber optic cable caused by irregularities in the shape of the***

fiber optic cable and the core. The condition is amplified by the temperature and splicing where one irregular piece of the fiber is splice to another piece.

This condition occurs when light rays transmitted down the center of the core travel faster than those that travel closer to the edge thereby distorting the information when it gets to the end of the cable.

FDDI: - FIBRE DISTRIBUTD DATA INTERCONNECT (INTERFACE)

One of the chief disadvantages of the token ring network is its failure. Failure of a single machine can disable the entire network. Then ring hardware is designed to avoid such problem but it becomes too complicated and costly and it is difficult to establish the proper communication.

To avoid this, another ring technology is used. It is called FDDI (fiber distributed data interconnect). It is 8 times faster than IBM token ring network and 10 times faster than the original Ethernet. To provide such high data rate FDDI uses optical fibers to interconnect computers instead of copper cables.

To overcome the failure it contains two complete rings. One that is used to send the data when everything is working correctly and another that is used only when the first ring fails.

the ring in an FDDI network are called ***counter rotating*** because data flows around the s4cond ring is opposite the direction of data flow around the main ring.

To understand the motivations for counter rotating ring consider how failure occurs:

If one station is failed and if data always passes in the same direction across both rings then disconnecting (failure) one station from the ring will prevent other station from communicating with each other. But if data travels in reverse direction across the second ring, the remaining stations can configure the network to use the reverse path.

So normally, one ring is used as shown in figure (a). A station always transmits and receives frames on the outer ring. When hardware detects the

failure or disconnection and reconfigure, they loop incoming bits back along the reverse path. Thus the failed station is removed and remaining stations are connected by the outer ring. This *process of reconfiguring to avoid a failure is called* ***self-healing network*** *(the network that detects the failure and recovers it automatically)*. After a station fails the neighbor station uses the reverse path to form a closed ring.

ROUTING PROTOCOLS

A routing protocol is a protocol that is used to exchange information among computers which enable them to build and maintain their routing tables. New paths are added or paths are deleted and cannot be used. Messages are sent among computers using the routing protocols.

It can be useful to know all possible routes to a given destination. However, a network gets quite large, so knowing all possible routes becomes impractical, as there are simply too many possible routes. So, one routing protocol can't handle the task of updating the routing tables of all routers. For this reason the network is divided into autonomous systems.

An autonomous system is simply a network operated by one organization. It is a group of networks and routers under the authority of a single administration. So the routing is divided into two parts:

1. Interior Routing
2. Exterior Routing

Interior Routing: Routing inside autonomous systems is referred to as interior routing.
Exterior Routing: Routing between autonomous systems is referred to as exterior routing.

Each autonomous system can choose an interior routing protocol to handle routing inside the autonomous system. However one exterior routing protocol is used to handle routing between autonomous systems.

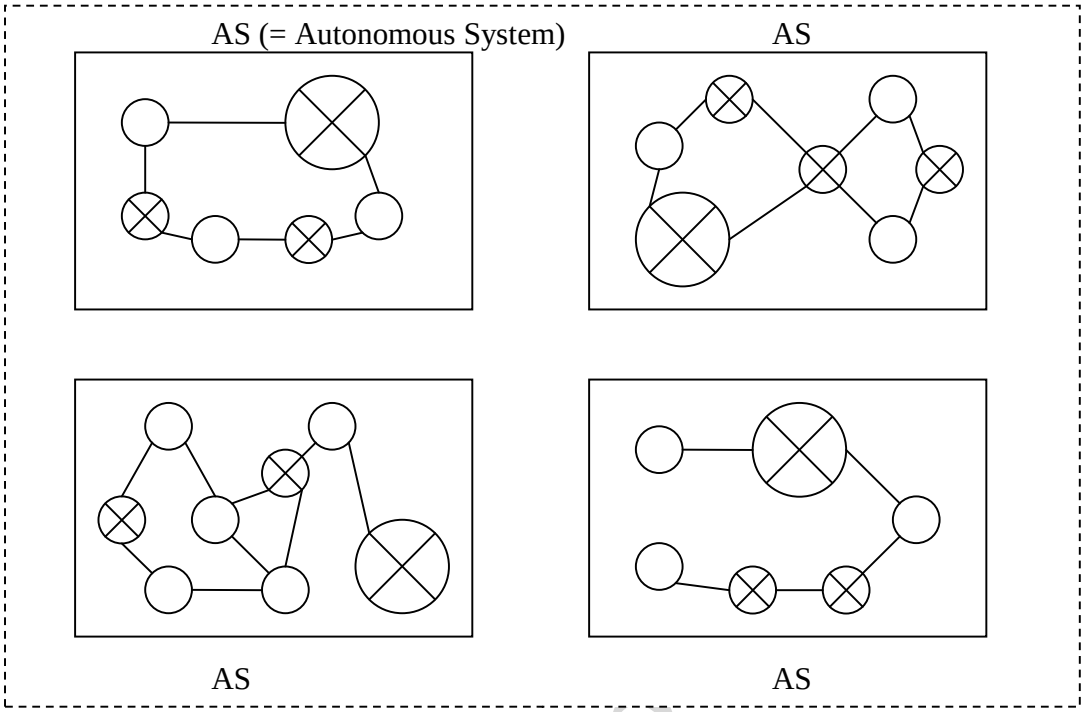


Fig (a)

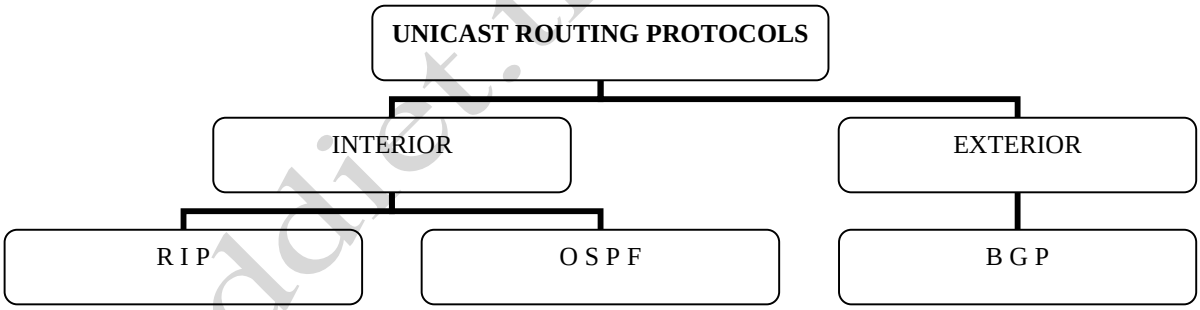


Fig (b)

As shown in fig (a), routers R1, R2, R3 and R4 use an interior and exterior routing protocol. The other routers use only interior routing protocol. The solid lines show the communication between routers that use interior routing protocols. The broken lines show the communication between the routers that use exterior routing protocols.

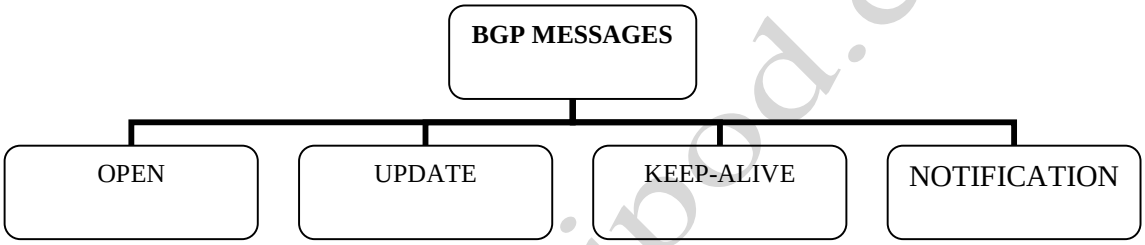
RIP → Routing Information Protocol
OSPF → Open Shortest Path First
BGP → Border Gateway Protocol

} Unicast Routing Protocol

ICMP → Internet Control Message Protocol
IGMP → Internet Group Management Protocol } Multicast Routing Protocol
EIGRP → Enhanced Interior Gateway Routing Protocol

1. **BGP (BORDER GATEWAY PROTOCOL):** It is a dynamic exterior routing protocol used on the internet to exchange routing information between autonomous systems. BGP is fundamentally a distance vector protocol. Pairs of BGP routers communicate with each other by establishing TCP connections.

   BGP uses four different types of messages:



Open Message: To create a neighborhood relationship, a router running BGP opens connection with a neighbor and sends an open message. If the neighbor accepts the neighborhood relationship, it responds with a keep-alive message which means that a relationship has been established between the two routers.

Update Message: It is the heart of the BGP protocol. It is used by a router to withdraw destinations that have been advertised previously, announce a route to a new destination. The BGP can withdraw several destinations but it can only advertise one new destination in a single update message.

Keep-Alive Message: The routers running the BGP protocols exchange keep-alive messages regularly (before their hold time expires) to tell each other that they are alive.

Notification Message: It is sent by a router whenever an error condition is detected or a router wants to close the connection.

2. **EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL):** It is a dynamic link state interior routing protocol. It is commonly used inside the organizations. EIGRP records information about a route's transmission capacity delay, reliability and load. EIGRP is unique in that computer or

routers store their own routing table as well as the routing tables for all of their neighbors, so they have a more accurate understanding of the network.

3. **RIP (ROUTING INFORMATION PROTOCOL):** The routing information protocol is an interior routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing.

   In this, every router keeps or maintains a routing table. This table has one entry for each destination network of which the router is aware. The entry consists of the destination network address, the shortest distance to reach the destination in hop count and the next router to which the packet should be delivered to reach its final destination.

   This routing table is updated upon receipt of a RIP response message. For this, an algorithm is used. This procedure is shown in fig (a) below.

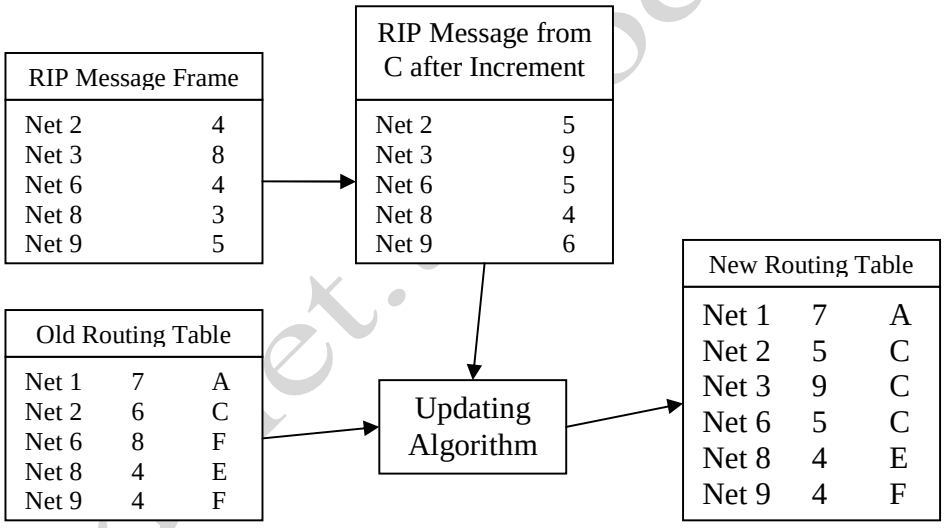


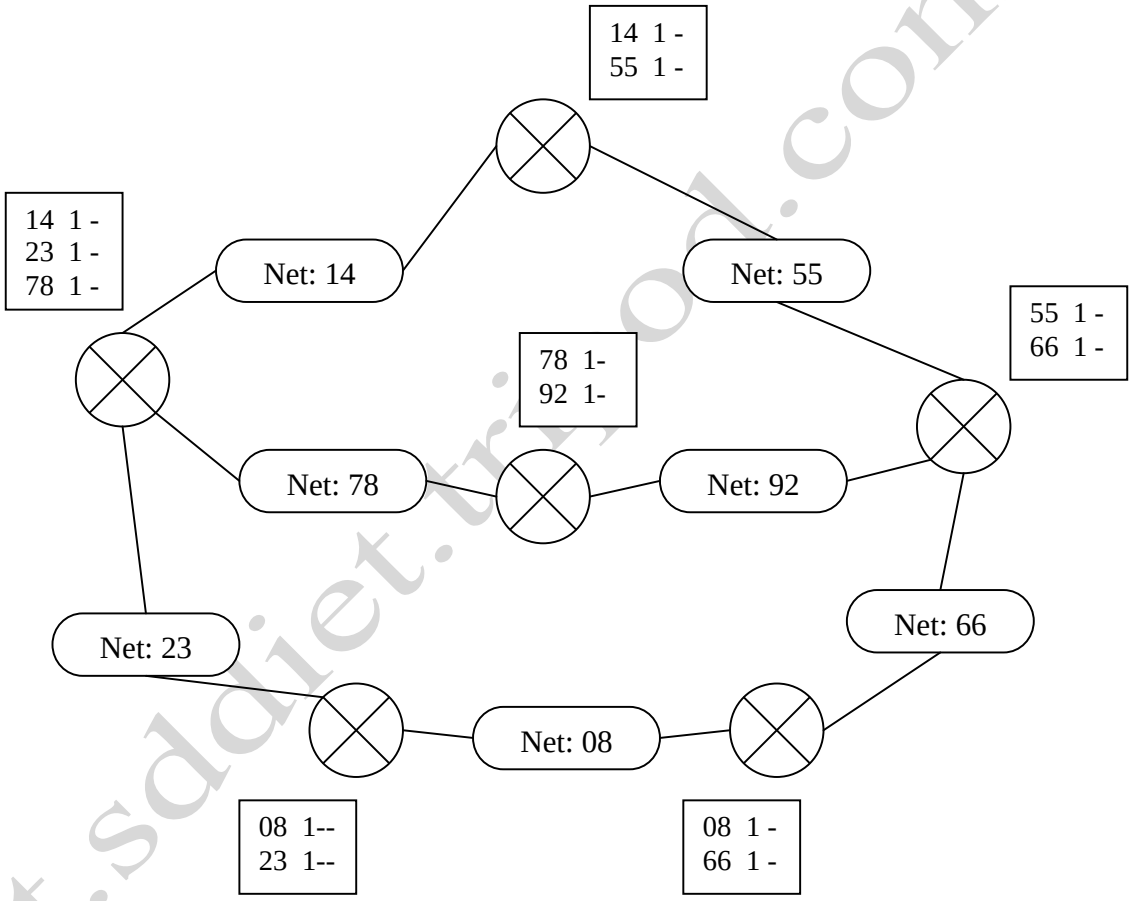
Fig (a)

Net 1: No news, do not change.
Net 2: Same, next hop, replace.
Net 3: A new router, add it.
Net 6: Different next hop, new hop, count smaller replace.
Net 8: Different next hop, new hop, count same, do not change.
Net 9: Different next hop, new hop, count larger, do not change.

Fig shows that a router receives a RIP message from router C. the message lists and consists of destination networks and their corresponding hop counts. The first step according to update routing algorithm is to increase the hop count by 1. This updated packet and old routing table are compared. The result is a

routing table with an up to date count for each destination. For Net 1, there is no new information, so the Net 1 entry remains the same.

In RIP when a router is added to a network, it initiates a routing table for itself. The table contains only the directly attached networks and the hop counts, which are initialized to 1. The next hop field, which identifies the next router, is empty. Fig (b) identifies the initial routing tables in a small autonomous system.



So each routing table is updated upon receipt of RIP message using RIP updating algorithm.

4. **OSPF (OPEN SHORTEST PATH FIRST):** It is also an interior gateway routing protocol. Its domain is also an autonomous system. This algorithm had to be published in the open literature, hence the "O" in "OSPF".

   OSPF supports three kinds of connections in networks:

(i) Point to point lines between exactly two routers.
(ii) Multi-access network with broadcasting (e.g. most LAN's)
(iii) Multi-access network without broadcasting.

A multi-access network is one that can have multiple routers on it, each of which can directly communicate with all the others. All LAN's and WAN's have this property. Fig (a) shows an AS containing all three kinds of networks.

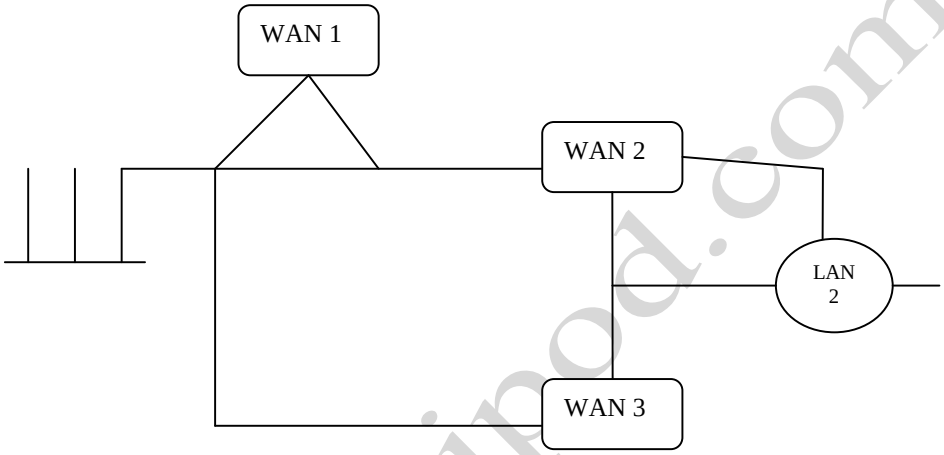


Fig (a)

OSPF operates by abstracting the collection of actual networks, routers and lines into a directed graph in which each arc is assigned a cost. It then computes the shortest path based on the weights on the arcs. A serial connection between two routers is represented by a pair of arcs, one in each direction. Their weights may be different. A multi-access network is represented by a node for the network itself plus a node for each router.
Fig(b) shows the graph representation of the network.

OSPF fundamentally represents the actual network as a graph like this and then computes the shortest path from every router to every other router.

Many of the AS's in the internet are very large. OSPF allows them to be divided into numbered areas, where an area is a network or a set of contiguous networks. Areas do not overlap but need not be exhaustive i.e. some routers may belong to no area. An area is a generalization of a subnet. Outside an area, its topology and details are not visible.

Every AS has a backbone area called area O. all areas are connected to the backbone by tunnels so it is possible to go from any area in the AS to any other area in the AS via the backbone. A tunnel is represented in the graph as an arc and has a cost. Each router that is connected to two or more areas is a part of the backbone. As with other areas, the topology of the backbone is not visible outside the backbone.

Within an area, each router has the same link state database and runs the same shortest path algorithm. Its main job is to calculate the shortest path from itself to every other router in the area, including the router that is connected to the backbone, of which there must be at least one. A router that connects to two areas needs the databases for both areas and must run the shortest path algorithm for each one separately.

During normal operation, three kinds of routers may be needed:
(i) Intra- Area
(ii) Inter- Area
(iii) Inter- AS
(iv) Backbone Router

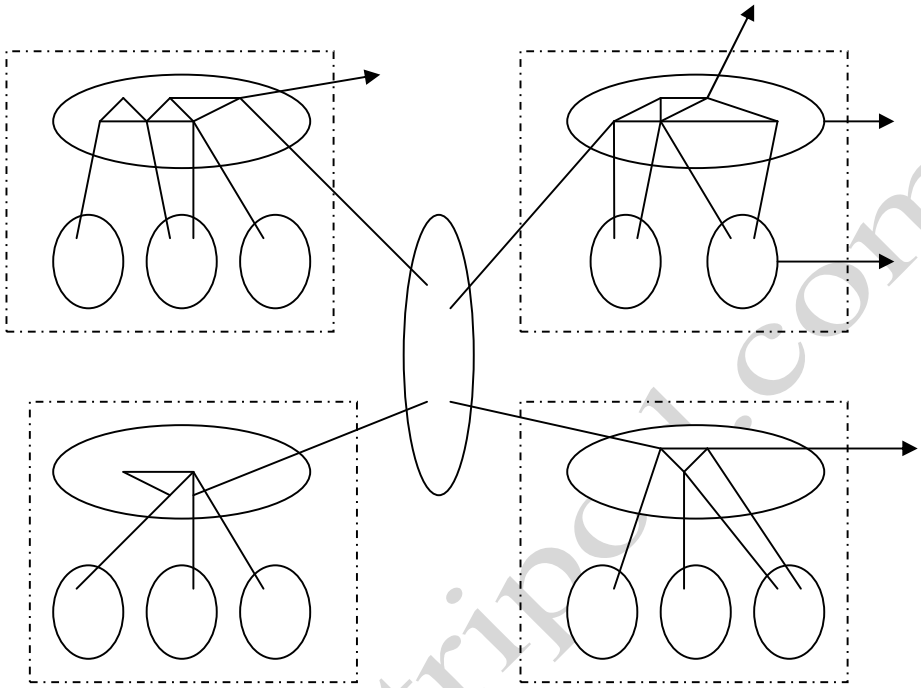
Intra-area routes are the easiest, since the source router already knows the shortest path to the destination router.

Inter-area routing always proceeds in three steps:
(a) Go from the source to the backbone
(b) Go across the backbone to the destination area
(c) Go to the destination

OSPF distinguishes four classes of routers:
1. Internal routers are wholly within one area.
2. Area border routers connect two or more areas.
3. Backbone routers are on the backbone.

4. AS boundary routers talk to routers in other AS's.

Figure shows part of the internet with AS's and area:



The routers can communicate with each other by five types of messages:

MESSAGE TYPE	DESCRIPTION
Hello	Used to discover who the neighbors are
Link State Update	Provides the senders' costs to its neighbors
Link State Acknowledgement	Acknowledges link state update
Database Description	Announces which updates the sender has
Link State Request	Requests information from partner

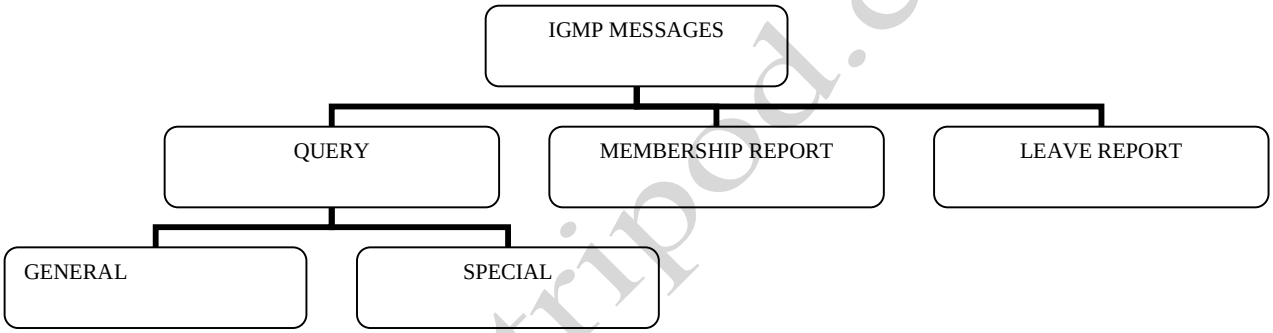
So OSPF works by exchanging information between routers. It is inefficient to have every router on a LAN talk to every other router on the LAN. To avoid this situation, one router is adjacent to all the other routers on its LAN and exchanges information with them.

5. **IGMP (INTERNET GROUP MANAGEMENT PROTOCOL):** It is a protocol that manages group membership. In any network there are one or more multicast routers that distribute multicast packets to hosts or other routers. IGMP gives the multicast router information about the membership status of hosts or routers connected to the network.

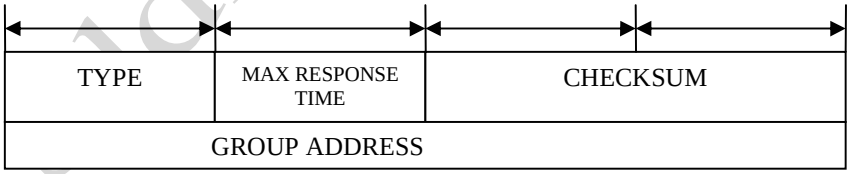
A multicast router may receive thousands of multicast packets everyday for different groups. If a router has no knowledge about the membership status of the hosts, it must broadcast all these packets. This creates a lot of traffic and consumes bandwidth. A better solution is to keep a list of groups in the network for which there is at least one loyal member. IGMP helps the multicast router create and update this list.

It has three types of messages:

(i) The Query Message
(ii) Membership Report
(iii) Leave Report



IGMP MESSAGE FORMAT:



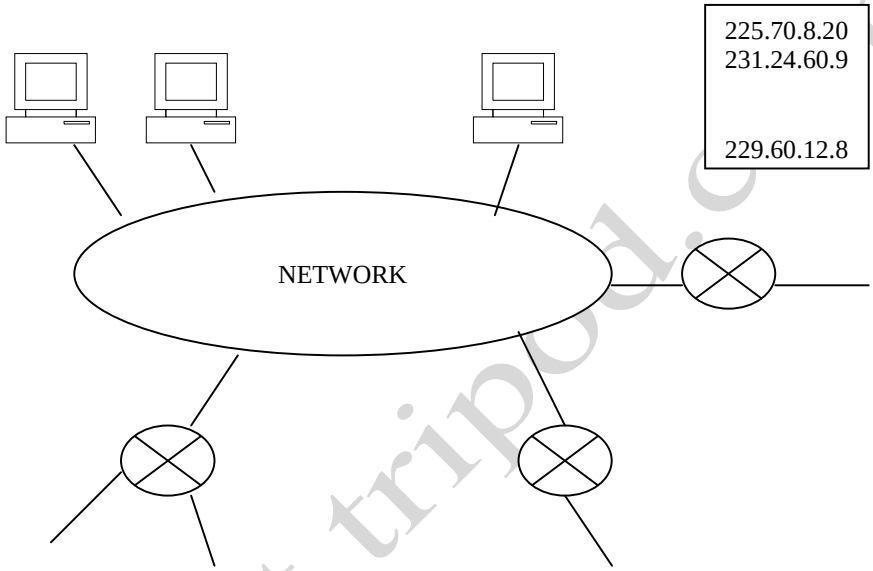
Type: This 8 bit field defines the type pf message. Type includes leave report, membership report and query message.

Maximum Response Time: This 8 bit field defines the amount of time in which a query must be answered.

Checksum: This is a 16 bit field carrying the checksum. The checksum is calculated over 8 bit message.

Group Message: The value of this field is 0 for a general query message. The value defines the group id in the special query, the membership report and the leave report messages.

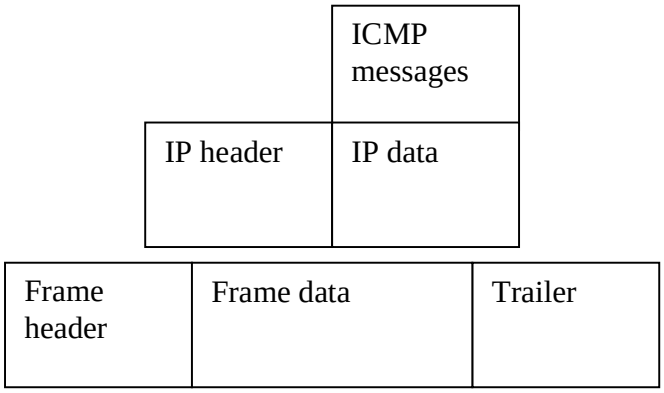
IGMP OPERATION: IGMP operates locally. A multicast router connected to a network has a list of multicast addresses of the groups for which the router distributes packets to group with at least one loyal member in that network.



For each group there is one router which has the duty of distributing the multicast packets destined for that group. This means that if there are three multicast routers connected to the network, there list of group_ids are mutually exclusive. For example in the figure only router R distributes packets with the multicast address of 225.70.8.20

A host or multicast router can have membership in a group. When a host has membership it means that one of its processes receives multicast packets from some group. When a router has a membership, it means that a network connected to one of its other interfaces receives these multicast packets.

6**) ICMP (INTERNET CONTROL MESSAGE PROTOCOL):** ICMP is a network layer protocol. Its messages are not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagram before going to the lower layer as shown in figure.



The value of the protocol field in the IP datagram is 1 to indicate that IP data are an ICMP message. ICMP messages are divided into two broad categories:

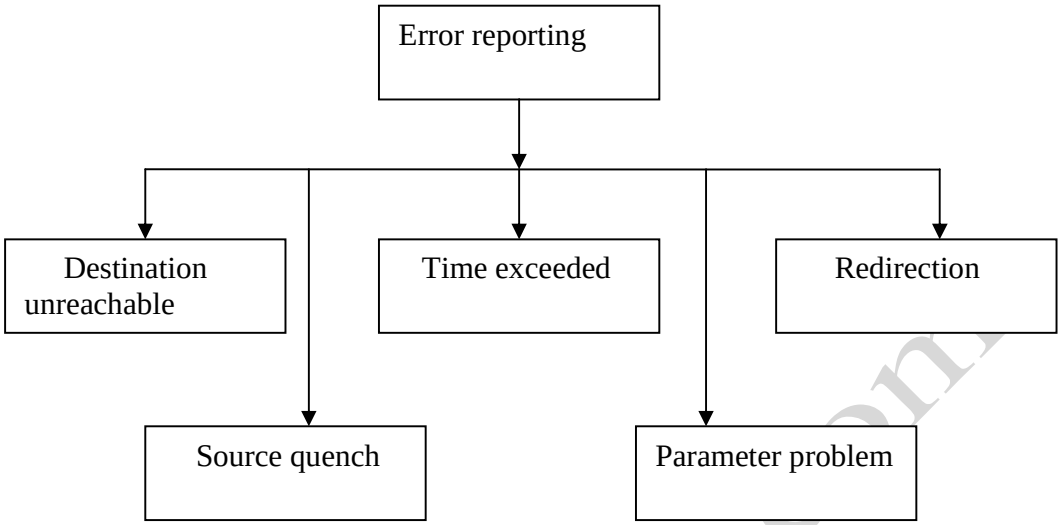
(1) error reporting messages

(2) query messages

1) ERROR REPORTING MESSAGES:

One of the ***main responsibilities*** of ICMP is to ***report errors***. **IP** is an **unreliable** protocol. This means that error checking and error control are not a concern of IP. ICMP was designed to compensate for this short-coming. ICMP does not correct errors, simply reports them. Error correction is left to higher level protocols. *Error reporting messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP address.* ICMP uses the source IP address to send the error message to the source of the datagram.

Five types of errors handled are:



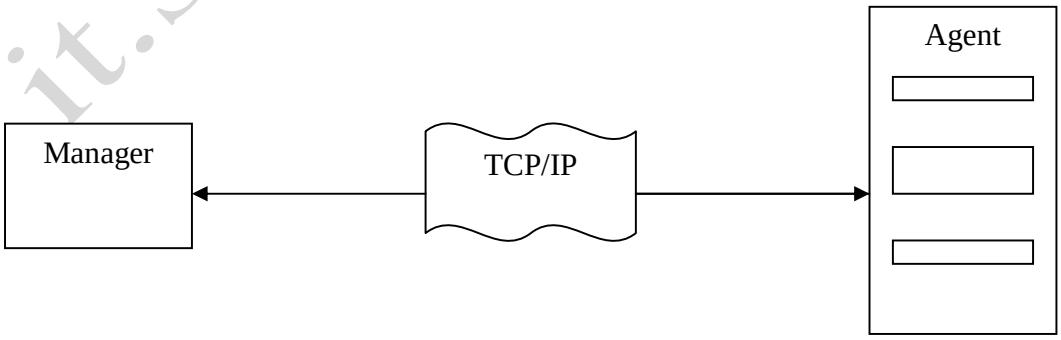
2) QUERY MESSAGES:

In addition to error reporting ICMP can diagnose some network problems. This is accomplished through the query messages. It is a group of 4-different pair of messages.

SNMP (Simple Network Management Protocol)

It is a framework for managing devices in an internet using TCP\IP protocol. It provides a set of fundamental operations for monitoring and managing an internet.

Concept:-it uses the concept of manager and agent that is manager, usually a host that controls and monitors a set of agents, usually routers.



SNMP is an application level protocol in which a few manager station controls a set of agents. The protocol is designed at the application level so that it can monitor devices made by diff. Manufacturers and installed on different physical network. So, it can be used in diff. Networks made up of diff. LAN's and WAN's connected by routers or gateways made by diff. Manufacturers.

Managers and Agents:-

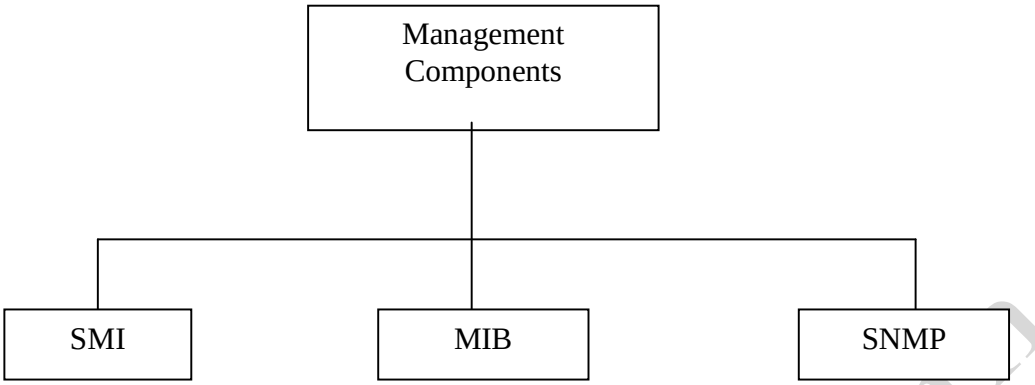
A management station called a manager is a host that runs the SNMP client program. A managed station called an agent is a router that runs the SNMP server program. Management is achieved through simple interaction b\w a manager and an agent.

The agent keeps information in a database. The manager has access to the values in a database. For example: - a router can store in appropriate variables the no. of packets received and forwarded. The manager can fetch and compare the values of these variables to see if the router is congested or not.

The manager can also make function so the router perform certain actions. For example: - a router periodically checks the values of a reboot counter to see when it should reboot itself. For example:-it reboots itself if the value of counter is zero. The manager can use this feature to reboot the agent remotely at any time. It simply sends a packet to force a 0 value in counter.

The agent can also contribute in management process. The server program running on the agent can check the environment and if it notices something unusual it can send a warning message to the manager.

COMPONENTS:



Structure of management Information

management information base

The management consists of another two more protocols SMI & MIB. SNMP uses the services provided by these two protocols to do its job. So, management is a team effort by SMI, MIB & SNMP.

SMI:-

It is a component used in N\W management. Its function is to name objects, to define the type of data that can be stored in an object and to show how to encode data for transmission over the N\w.

MIB:-

It is the second component used in a N\W management. Each agent has its own MIB which is a collection of all the objects that the manager can manage.

SNMP:-SNMP define 5 messages:-

1. **get request**
2. **get next request**
3. **set request**

4. **get response**
5. **trap**

I) Get Request:-

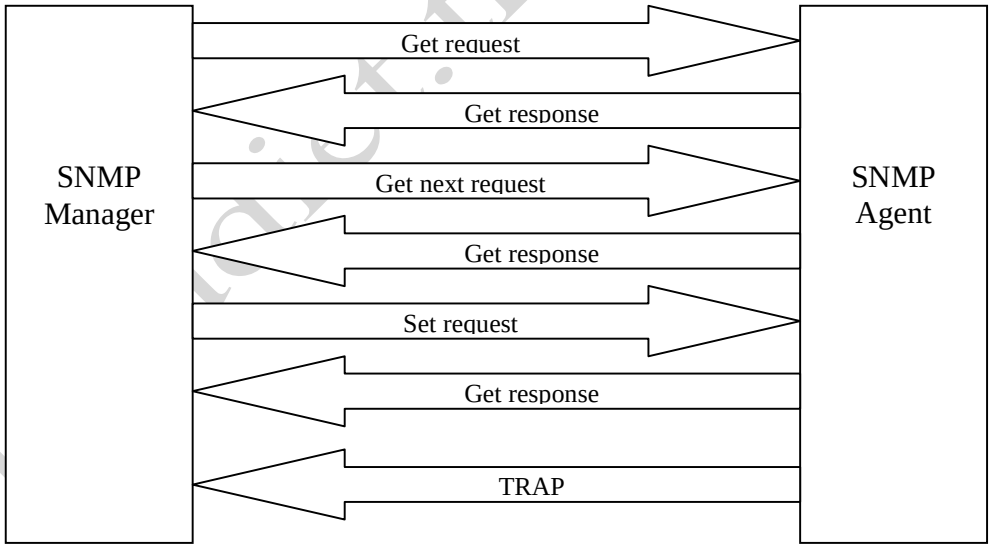
This is a message from the manager to the agent to retrieve the value of a variable.

II) Get next Request:-

It is sent from manager to the agent to retrieve the value of a variable. The retrieved value is the value of the object following the defined object in the message. It is mostly used to retrieve the values of the entries in table.

III) Get Response:-

This message is sent from an agent to the manager in response to get request and to get next request. It contains the values of the variables requested by the manager.



UDP CONNECTIONS

IV) Set Request:-

This message is sent from the manager to the agent to store a value in a variable.

V) TRAP:-

This message is sent from agent to manager to report for an event. For example:-if the agent is rebooted, it informs the manager and reports the time of rebooting.

SIGNALING

To establish a telephone call a series of signaling messages must be exchanged. There are two basics types of signal exchange:-

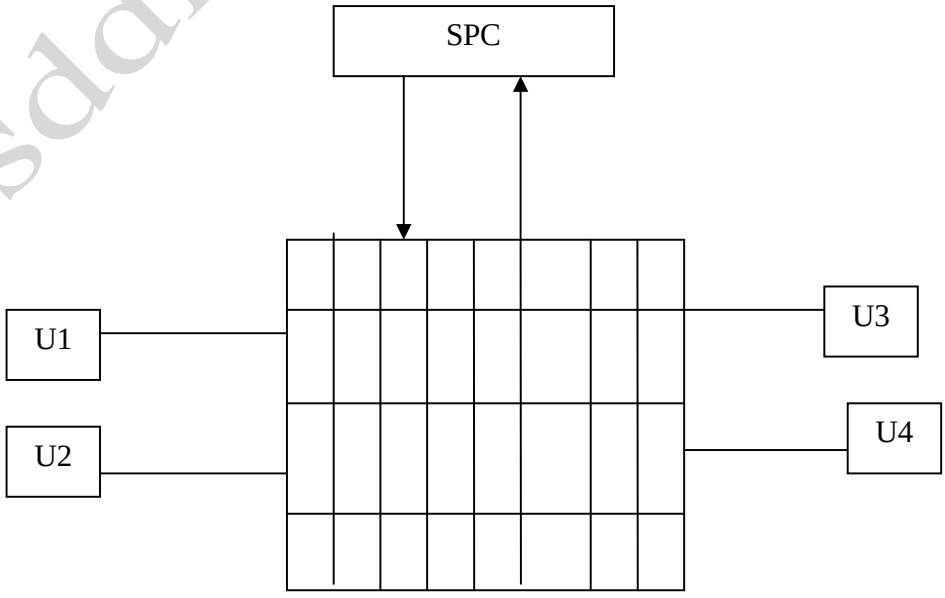
1. **Between user and N\w.**
2. **Within the N\W.**

Both types of signaling must work together to establish the call.

In general, the signaling message generate control signal that determine the configuration of switches i.e. the messages direct a switch to a state in which a given input is connected to the desired output.

In figure (i) traditional N\W signaling information would arrive in telephone lines and be routed to the control system. Initially, hard-wired electronic logic was used to process these signaling messages. The class of **stored program control (SPC)** switches emerged when computers were introduced to control the switch. With the help of SPC computer a request for a call would come in, a check would be made to see whether the destination is available and if so, the appropriate connection would be made.

FIGURE (i)



As shown in fig (ii) the setting up a call also required that computer controlling the switches communicate with each other to exchange the signaling information. A modem and separate communication lines were introduced to interconnect these computers.

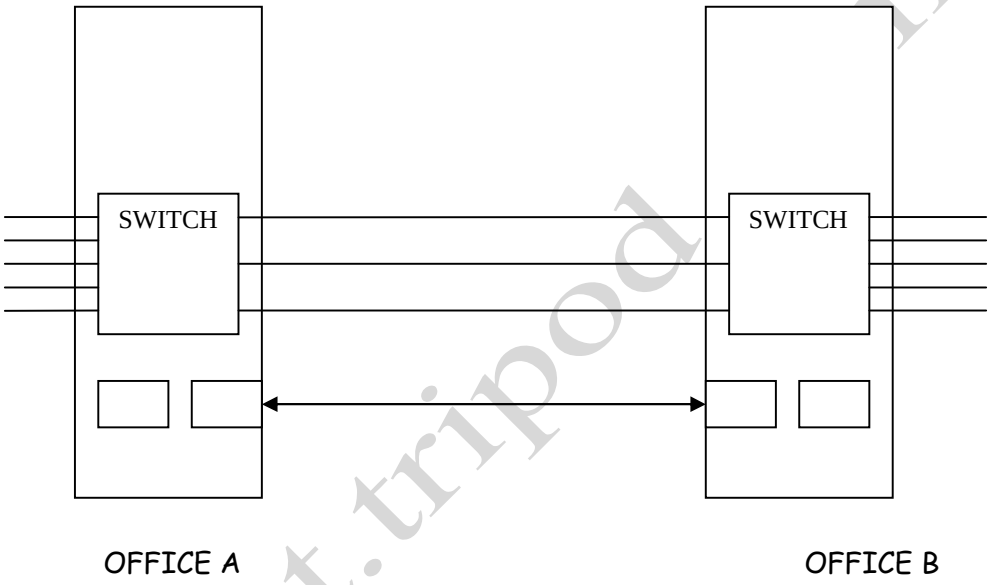


FIGURE (ii)

Now consider the operation of signaling N\W .Its purpose is to implement connectivity b\w the computer that control the switches in the telephone N\W by providing for the exchange of messages. Fig (iii) shows the telephone N\W. It consists of two parts:-

1. **<u>Signaling N\W:-</u>that carries the information to control the connection.**
2. **<u>Transport N\W:-</u>that carries the user information.**

Communications from the user are split into two streams at SSP (service switching point) the signaling information is directed towards the signaling N\W where it is

routed and processed as required. The signaling system then issues command to the switches to establish the desired connection.

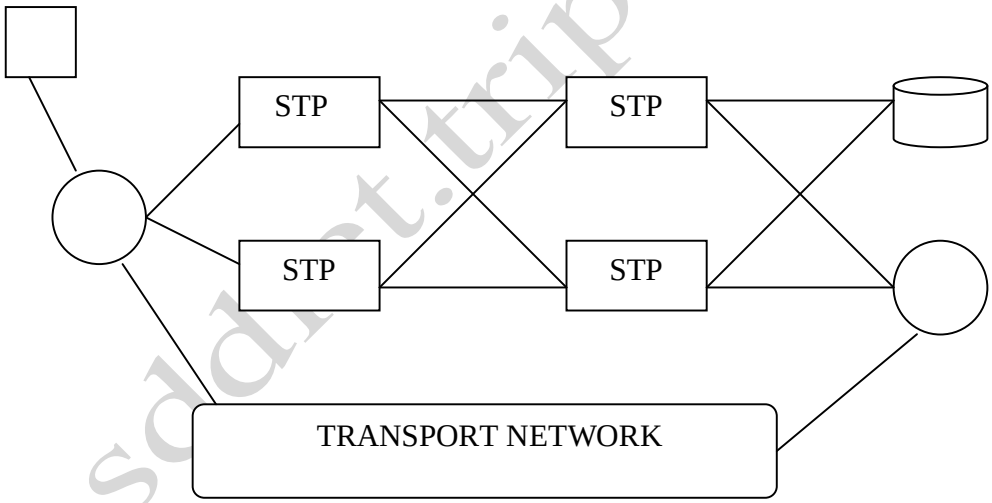
The second stream in SSP consists of the user information that is directed to the transport N\W where it flows from one user to the other.

The function of the signaling network is to provide communications between the computers that control the switches. The computers communicate through the exchange of discrete messages. The best way of implementing such a network is through a packet switching network that transfers information in the form of packets between network elements.

SSP----- Service switching point

STP----- Signal transfer point

SCP----- Service control point



Telephone companies use the term intelligent N\W to denote the use of advance signaling N\W that provide the number of services. These services include identification of calling person, screening out of callers, call back of previous caller, voice mail and others. For example:-N\W use the intelligent peripheral that provides all these services (SS7 N/W)

SIGNALING SYSTEM #7 ARCHITECTURE (SS7):-

The signaling system #7 (SS7) N\W is a packet network that controls the setting up managing and realizing of telephone calls. The N\W also provide support for intelligent N\W, mobile cellular N\W and ISDN. The ss7 network architecture is shown in fig.

This architecture use parts instead of layers. The message transfer part (MTP) corresponds to the lower three layers of OSI reference model. Level 1 of MTP corresponds to the physical layer of signaling links in the SS7 N\W.

MTP level 2 ensures that messages are delivered reliably across a signaling like MTP level 3 ensures that messages are delivered b\w signaling points across the SS7 N\W> Level 3 provides routing and congestion control that reroutes traffic away from failed links and signaling points.

ISDN user part (ISUP) protocol performs the basic set up management and release of telephone calls. The telephone user part (TUP) is used instead in some countries.

The SCCP allows these applications to be addressed by building on the MTP to provide connectionless and connection oriented service.

The TCAP part defines the messages and protocols that are used to communicate b\w application that used the SS7 N\W. The TCAP uses the connectionless service provided by the SCCP to support database queries that are used in intelligent N\W.

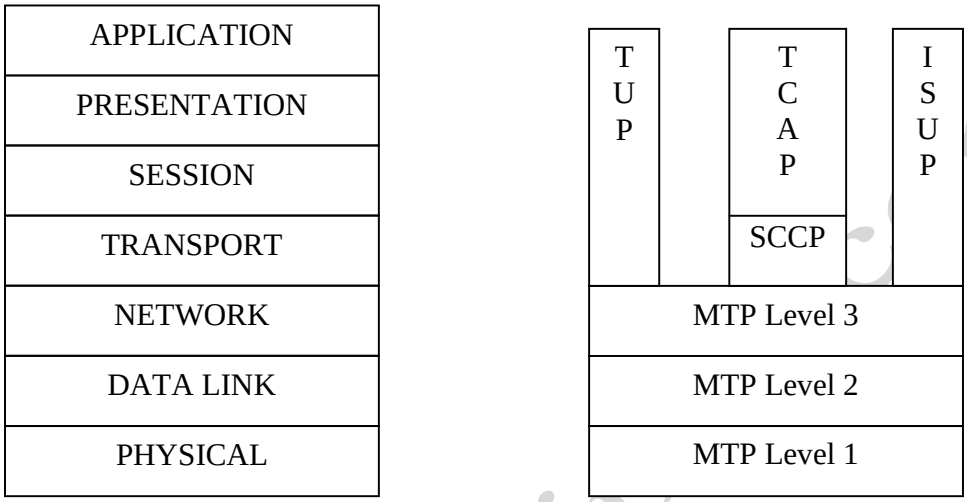
TUP----- telephone user network

TCAP----transaction capabilities part

ISUP------ISDN user part

SCCP-----signaling connection control part

MTP------ message transfer part



TCP (Transmission Control Protocol)

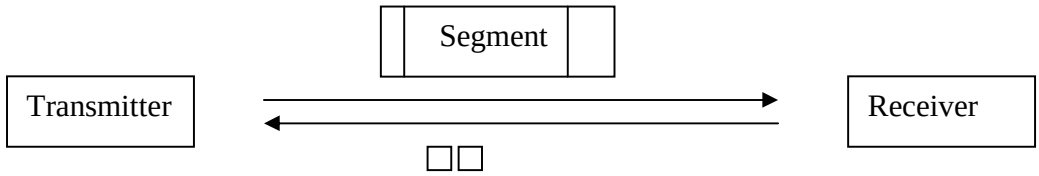
TCP Reliable Stream Service :->

TCP provides a logical **full duplex** connection b/w two application layer processes. TCP provides these application processes with a **connection oriented, reliable, in-sequence, byte stream** service. TCP also provides a **flow control** that allows receivers to control the rate at which the sender transmits information.

Before data transfers can begin, TCP establishes a connection between the two application processes by setting up variables. These variables are stored in a connection record that is called the **transmission control block (TCB).** Once, the connection is established, TCP delivers data over each direction in the connection correctly & in sequence. To implement reliability TCP uses a form of selective repeat ARQ. TCP terminates each direction of the connection independently allowing data to continue flowing in one direction after the other direction has been closed.

TCP Operation :->

TCP is used to provide a ***connection oriented, reliable, stream*** service. User is interested to deliver the information so that it is error free, without duplication and in the same order it was produced by the sender. We assume that the user information consist of a stream of bytes as shown in fig. For ex. for the transfer of a long file the sender insert a byte stream into the transmitter's send buffer the task of TCP is to ensure the transfer of the byte stream to the receiver & the orderly delivery of the stream to the destination application.



The IP provides a connectionless packet transfer service so different packets can traverse a different path from same source to the same destination & can arrive out of order. Therefore in the internet the old messages from the previous connections may arrive at the receiver, so complicating the task of eliminating duplicate messages. TCP deals with this problem using the method of sequence no.

The transmitter arranges a consecutive string of bytes into a PDU that is called a segment. The segment contains a header. This segment also contains a sequence no which corresponds to the no of first byte in the string that is being transmitted.

The other major operation is the use of **push command**. Transmitter decides to transmit a segment when the no of bytes in the send buffer exceeds some specified threshold or when a timer that is set periodically expires. The sending application can also use a push command that forces the transmitter to send a segment.

When a segment arrives, the receiver performs an error check to detect transmission error. If the segment is error free and is not a duplicate segment then the bytes are inserted into the appropriate location in the receive buffer.

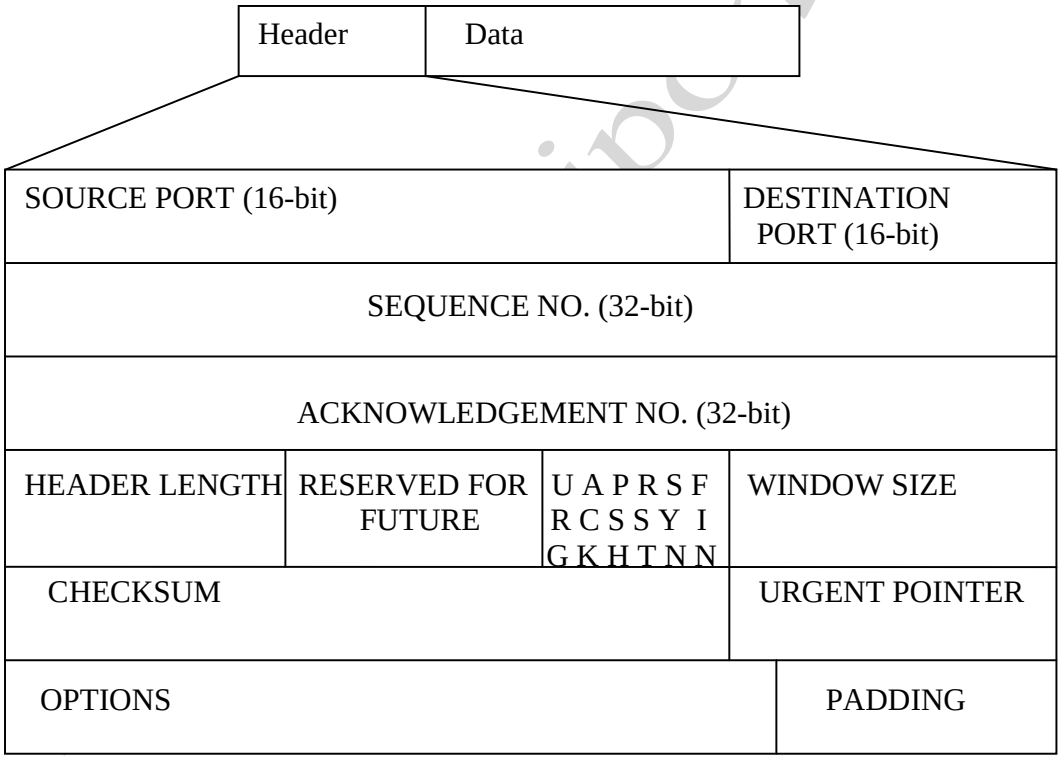
The next operation is the **flow control**. The flow control function is implemented through an advertised window field in the segment header. Segments

that travel in the reverse direction contain the advertised **window** size that informs the transmitter the no. of buffers currently available at the receiver.

TCP Protocol :->

It consists of TCP segment, TCP checksum, TCP connection, data transfer & TCP connection termination.

TCP Segment;--***Fig shows the format of TCP segment-***



Source port and destination port no. - The source ports & destination ports identify the sending and receiving application respectively. These are 16-bit fields.

Sequence No.- This is 32 bit field and it defines the position of data in the original data stream because the data stream is divided in 2 or more TCP segments.

Acknowledgement No—it is 32 bit field. It is used to acknowledge the receipt from the other communicating device. This ACK No. is valid only if ACK bit in the control field is set. If the ACK bit is not set then this ACK field is meaningless. Once the connection is established the ACK bit must be set.

Header length---This field specify the length of the TCP header in 32 bit words. This information allows the receiver to know the beginning of the data area.

Reserved---It is a 6 bit field & is reserved for future use & and must be set to 0.

URG (Urgent) ---If this bit is set the urgent pointer, field is valid otherwise not. This bit indicates that the data in segment are urgent.

ACK.(Acknowledge)---- If this bit is set the acknowledgement no. field is valid otherwise not.

PSH. (PUSH)----When this bit is set, it tells receiving TCP module to pass or push the data to the application immediately.

RST (Reset)-----When this bit is set it tells the receiving TCP module to abort the connection because of some abnormal condition.

SYN (Synchronization) ---- This bit is used for seq. no. synchronization in three types of segments—

1) Connection req.
2) Connection conformation. (With ACK. Bit set).

3) Confirmation Acknowledgement (with the acknowledgement bit set)

FIN (Finish) ----When this bit is set it tells the receiver the sender does not have any more data to send. So FIN bit is used in the connection termination in three types of segments—

1) Termination reg.
2) Termination conformation.(with ACK bit set)
3) Acknowledgement of termination conformation(with ACK bit set)

Window size----It is a 16 bit field. It specifies the number of bytes the sender is willing to accept .This field can be used to control the flow of data and congestion.

Checksum----It is used in error detection. It is also a 16-bit field.

Urgent pointer. --- It is a 16-bit field and is valid only if URG bit is set to 1. In this case the sender is informing the receiver that there are urgent data in data portion of the segment. This pointer defines the end of urgent data & start of the normal data.

Options---- The option field may be used to provide other information that are not covered by the header .If the length of option field is not a multiple of 32 bits, extra padding bits will be added .The most important option is used by a sender is to indicate the **maximum segment size (MSS)** it can accept .The times up option is also used for high speed connection.

TCP Checksum –The purpose of TCP checksum field is to detect the errors. The checksum computation procedure is simpler to that used to compute an IP checksum except for two features –

(1)-If the length of segment is not a multiple of 16 bits, the segment will be padded with zero's to make it a multiple of 16 bits .In doing so TCP length field is not modified.

(2)- Second a pseudo header is added to the beginning of the segment when performing the checksum computation. The pseudo header is created by the source & the destination host during the checksum computation & is not transmitted .This mechanism ensures the receiver that the segment has indeed reached the correct destination host and port and that the protocol type is TCP. At the receiver the IP add information in the IP packet that contained the segment is used in checksum calculation---

SOURCE IP ADDRESS		
DESTINATION IP ADDRESS		
00000000	PROTOCOL	TCP segment length

TCP Pseudo header

So TCP provide a connection oriented, full duplex connection. For this connection must be established, and data transfer take place after the connection should be release.

Connection Establishment :->

Before any host can send data a connection must be established. TCP establishes the connection using a three way handshake procedure as shown in fig. the handshake is described in following steps:

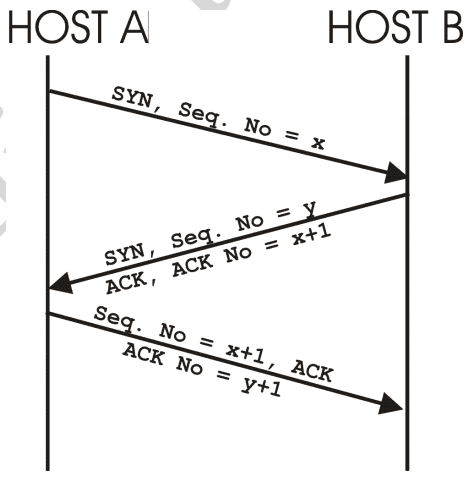
1. Host A sends a connection request to host B by setting the SYN bit. Host A also registers its initial seq. no. to use (seq. no=x)

2. Host B acknowledge the request by setting the ACK bit & indicating the next data byte to receive (ACK-no=x+1). At the same time , host B also sends a request by setting the SYN bit & registering its initial seq. no to use(seq. no=y)

3. Host A acknowledges the request from B by setting the ACK bit & confirming the next data byte to receive

(ACK no=y+1) note that the seq. no is set to x+1. On receipt at B the connection is established

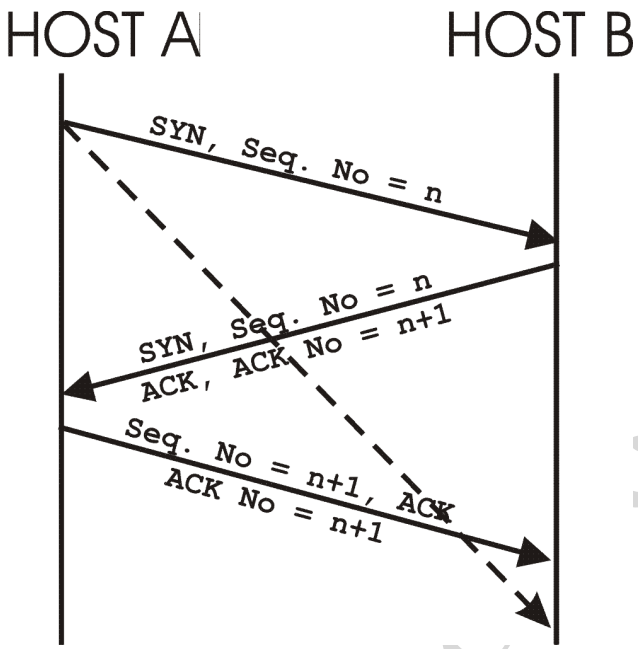
If during a connection establishment phase, one of the hosts decides to refuse a connection req., it will send a reset segment by setting the RST bit.



Because TCP segments can be delayed, lost & duplicated. So the initial seq. no should be different, each time when a host request for a connection.

To see why the initial seq. no must be different, consider a case in which a host can always use the same initial seq. no, say n, as shown in fig (ii)

Figure (ii)



Delayed segment with seq. no. =n+2 will be accepted

After a connection is established a delayed segment from the previous connection arrives. Host B accepts this segment, since the SEQ. no turns out to be legal. If a segment from the current connection arrives later, it will be rejected by the host B, thinking that segment is a duplicate. The Host B can't distinguish a delayed segment from the new one. So the initial segment no. is always unique.

DATA TRANSFER :->

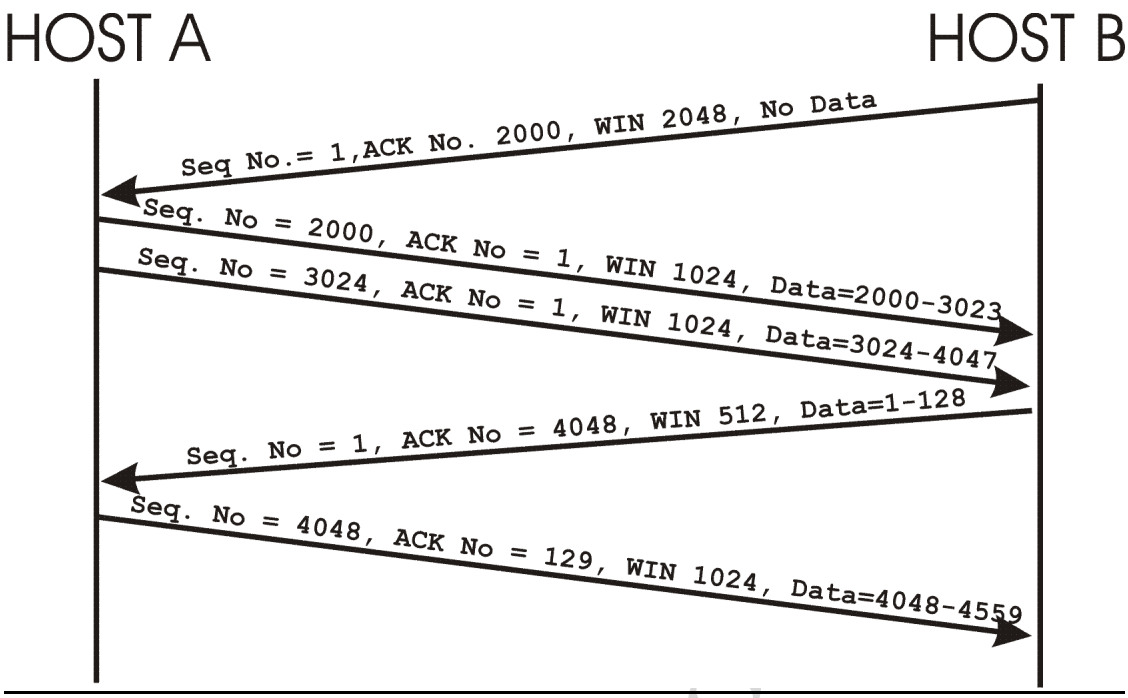
After the connection establishment the data will transfer. TCP also apply flow control over the connection by advertising the window size. It is the process of regulating the traffic b/w two points. Fig. shows an example how a TCP entity can control the flow of data. Suppose at time (t_o), the TCP module in

host B advertised a window of size 2048 & expected that the next byte received t_o a seq. no 2000. The advertised window allows host A to transmit up to 2048 bytes.

At time t_1, host A has only 1024 bytes to transmit all the data starting with a seq. no 2000. The TCP entity also advertises a window of size 1024 byte to host B. after some delay at time t_2; A has another 1024 byte of data & transmits it. After the transmission A's sending window close completely. It is not allowed to transmit any more data until acknowledgement comes back.

At time t_3 host B has 128 bytes of data to transmit, it also wants to acknowledge the first two segments of data from host A. Host B can simply 'Piggyback' the acknowledgement to the data segment. Also at this time host B finds out that it can allocate only 512 bytes of receive buffer space for this connection because other connection are also competing for the previous memory. When host A receive the segment, A changes its sending windows to 512 bytes as host B find out that it can allocate only 512 bytes of receive buffer space for this connection. So it shrinks the advertised window from 2048 bytes to 512 bytes.

If at time t_4 host A has 2048 bytes of data to transmit then it will transmit only 512 bytes. So the advertised windows dynamically control s the flow of data from the sender to the receiver.



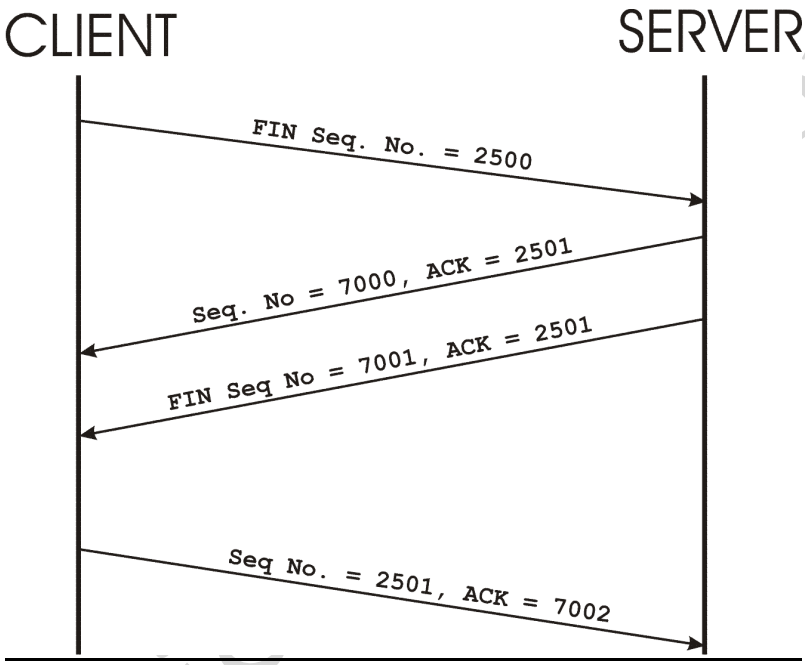
TCP Connection Termination : _>

A termination is initiated when application tells that it has no more data to send. The TCP entity completes transmission of its data & upon receiving the acknowledgement from the receiver issue a segment along with setting the FIN bit. Upon receiving the FIN segment a TCP entity informs its application that other entity has terminated its transmission of data. When connection in one direction is terminated, the other party can continue sending the data.

So, four steps are needed to close the connection in both directions as shown in fig.

1. The client sends the first segment a FIN segment as well as its own segment no.
2. The server TCP sends the second segment, an ACK segment, to confirm the receipt of FIN segment from the client.

3. The server TCP can continue sending data in the server-client direction. When it does not have any more data to send, it sends the third segment. This segment is a FIN segment.
4. The client TCP sends the fourth segment, an ACK segment to confirm the receipt of the FIN segment from the TCP server.

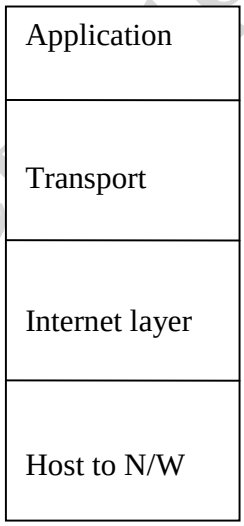


TCP/IP REFERENCE MODEL

When radio and satellite networks (connectionless services) were added then the existing protocols had trouble so new reference architecture was needed. So there was ability to connect multiple networks in a seamless way. The architecture that was developed for this is called ***TCP/IP model***. It is popular because of its two primary protocols.

It has **four** layers:

Figure (i)



(1) APPLICATION LAYER:

TCP/IP model does not *have* ***session*** *and* ***presentation layer***. The top layer is the application layer. It contains all the higher level protocols. They include *Virtual terminal (TELNET), FTP, SMTP* as shown in fig (ii)

The virtual terminal protocol allows a user on one machine to log on to a user onto a distant machine work there. The FTP provides a way to more data efficiently from

one machine to another. E-mail is just a kind of file transfer and SMTP is a protocol that was developed for . Many other protocols are added DNS, HTTP, and USENET etc.

(2) TRANSPORT LAYER:

The layer above the internet layer is called transport layer. Two end-to-end protocols have been defined here.

(i) TCP **(ii) UDP**

(i) **TCP:** it is ***transmission control protocol***. It is ***reliable, connector oriented*** protocol that allows a byte stream on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and possesses each one onto the internet layer. At the destination the receiving TCP processes reassembles the received messages into the output stream. TCP also handles flow control to make sure that a fast sender can't swap a slow receiver.

(ii) **UDP:** it is ***user datagram protocol.*** It is ***unreliable, connectionless*** protocol. It is used for those applications that do not want TCP's sequencing or flow control and wish to provide their own it is also used for requests, reply queries and applications in which prompt delivery is more important than accurate delivery.

(3) INTERNET LAYER:

It is similar to the ***network layer*** of the ***OSI model***. The job of internet layer is to inject packets into any network, have them travel independently to the destination. They may arrive even in different order than the way in which they were sent; in

that case it is the job of the higher layers to rearrange them, if in order delivery is desired.

The internet layer defines a protocol that is called ***Internet protocol (IP)*** and deals with the packets. The job of this layer is to deliver IP packets where they are supposed to go. Packet routing is major issue as to avoid congestion.

(4) HOST TO NETWORK LAYER:

Below the internet layer is a host to network layer. It adds the ***features of data link layer*** and ***the physical layer*** of the ***OSI model***. In this the host has to connect to the network using some protocol, so it can send IP packets to it.

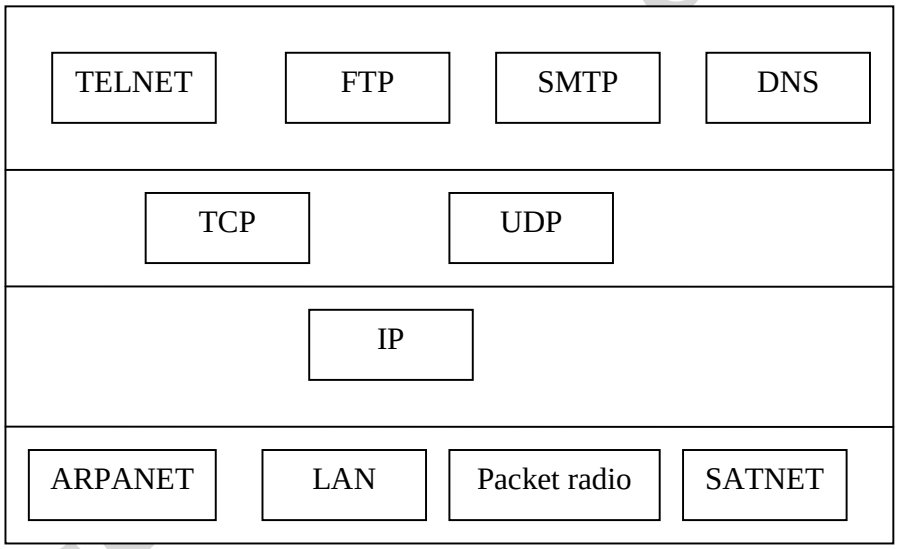


Figure (ii)

SUBNETTING

An IP address is 32 bit long. One portion of the address indicates a network (netid) and the other portion indicates the host (or router) on the network (hostid). So there is a two-level hierarchy in IP addressing. To reach a host on the internet, we must first reach the network using the first portion of the address i.e. netid. Then we must reach the host itself using the second portion (hostid). Classes A, B and C in IP addressing are designed with two-levels of hierarchy.

In many cases, the two levels of hierarchy are not enough. For example, imagine an organization with a class B address. The organization has two-level hierarchical addressing. But it cannot have more than one physical network as shown in fig (a).

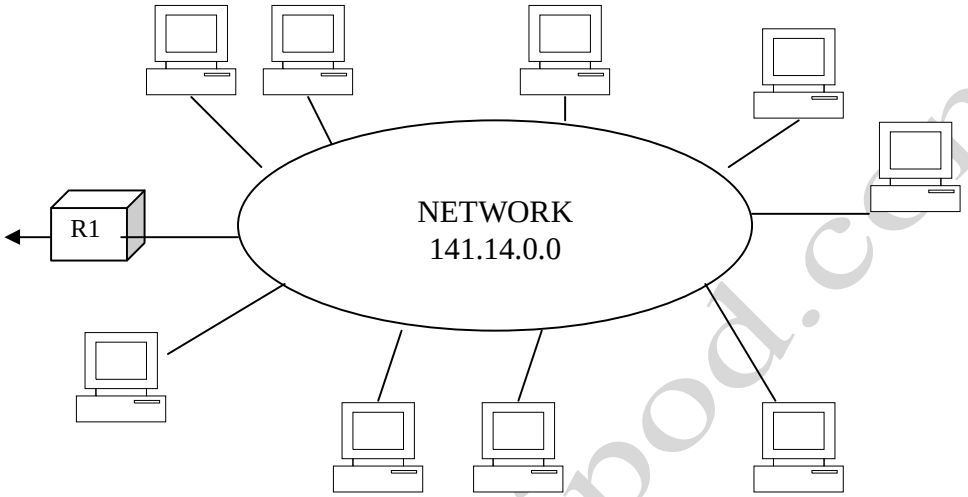
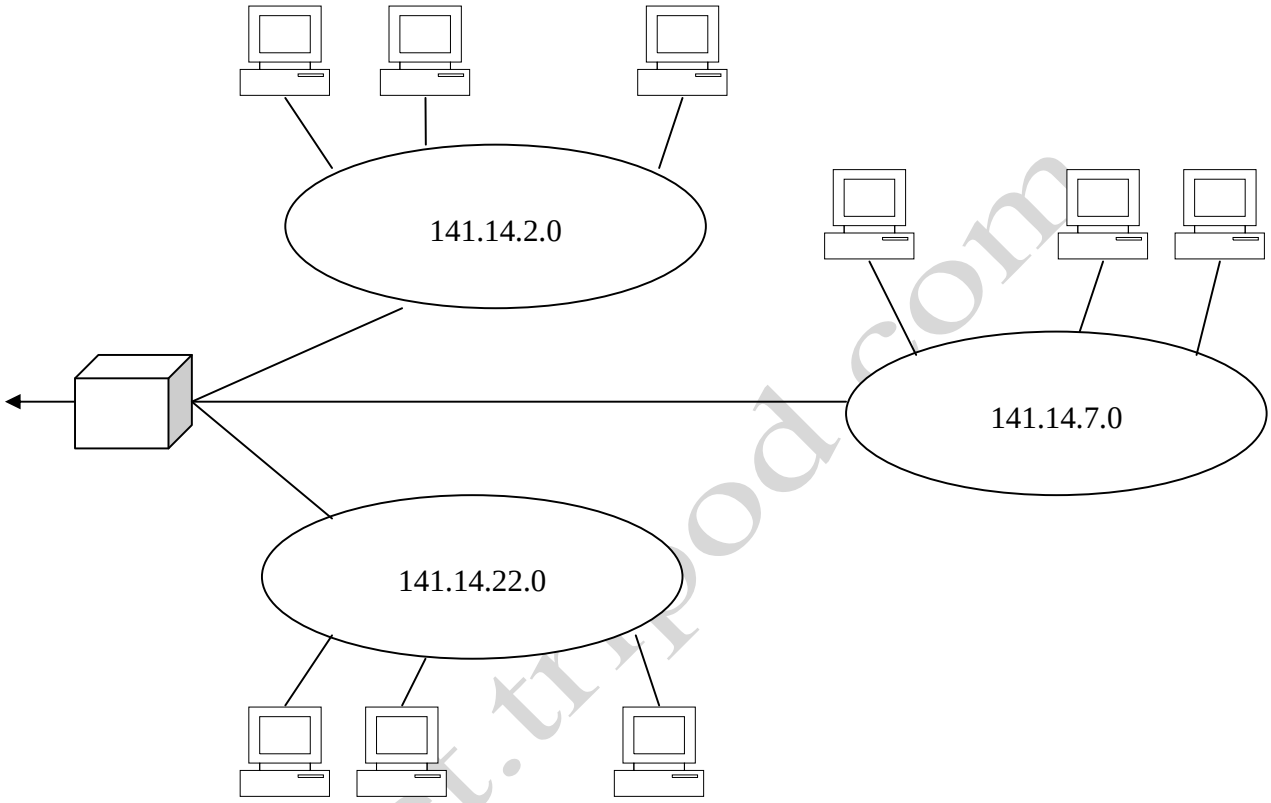


Fig (a)

With this scheme, the organization is limited to two levels of hierarchy. The hosts cannot be organized into groups, and all of the hosts are at the same level. The organization has one network with many hosts.
One solution to this problem is subnetting i.e. further division of a network into smaller networks called subnetworks.

Fig (b) on the next page shows the network which is divided into three sub networks.

A NETWORK WITH THREE LEVELS OF HIERARCHY (SUBNETWORKS)



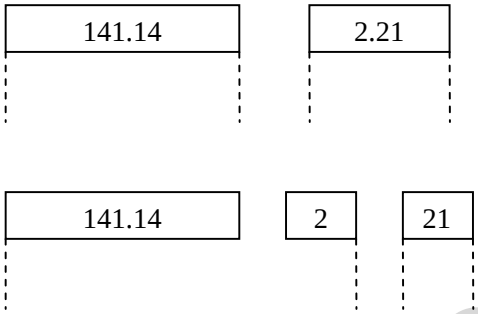
In this example, the rest of the internet is not aware that the network is divided into three physical subnetworks. The three subnetworks still appear as a single network to the rest of the internet.

A packet destined for host 141.14.2.21 still reaches router R1. The destination address of the IP datagram is still a class B address where 141.14 defines the netid and 2.21 defines the hostid.

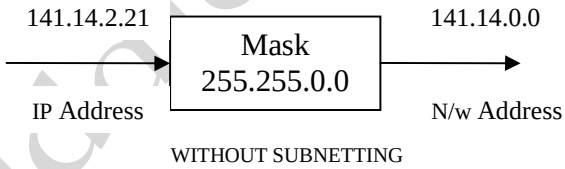
When the packet arrives at router R1, the interpretation of the IP address changes. Router R1 knows that the network 141.14 is physically divided into three subnetworks. It knows that the last two bytes define two things: subnetid and hostid. Therefore 2.21 must be interpreted as subnet 2 and hostid 21. The router R1 uses the first two bytes (141.14) as the netid, the third byte (2) as subnetid and the fourth byte (21) as the hostid.

THREE LEVELS OF HIERARCHY: Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system. Now we have three levels: netid, subnetid and hostid.

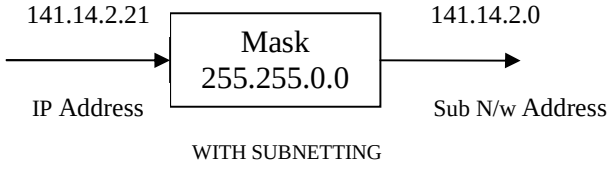
The netid is the first level. It defines the site.
The second level is the subnetid. It defines the physical subnetwork.
The hostid is the third level. It defines the connection of the host to the subnetwork.



SUBNET MASK: Masking is a process that extracts the address of the physical network from an IP address. Masking can be done whether we have subnetting or not. If we have not subnetted the network, masking extracts the network address from an IP address. If we have subnetted, masking extracts the subnetwork address from an IP address.



WITHOUT SUBNETTING



WITH SUBNETTING

When a router receives a packet with destination address, it needs to route the packet. The routing is based on the network address and subnetwork address. The router outside the organization routes the packet based on the network address, the router inside the organization routes the packet based on the subnetwork

address. The router outside the organization uses a default mask and the router inside the organization uses a subnet mask.

TCP/IP Architecture

TCP/IP refers to transmission control protocol & internet protocol. The application layer protocol such as FTP & HTTP sends messages using TCP. Application layer protocol such as SNMP & DNS sends their message using UDP. The PDU's (Protocol Data Units) exchange by the peer TCP protocols are called TCP segments or segments while those exchanged by UDP protocols are called UDP Datagrams or Datagrams. The PDUs Exchanged by IP protocols are called IP packets or packets. IP packets are sent to the N/W interface for delivery across the physical N/W. At the receiver packets passed by the N/W interface are demultiplexed to the appropriate protocol. The Receiving IP entity needs to determine whether a packet has to be sent to TCP or UDP. Finally, TCP (UDP) sends each segment (datagram) to the appropriate application based on the port no.

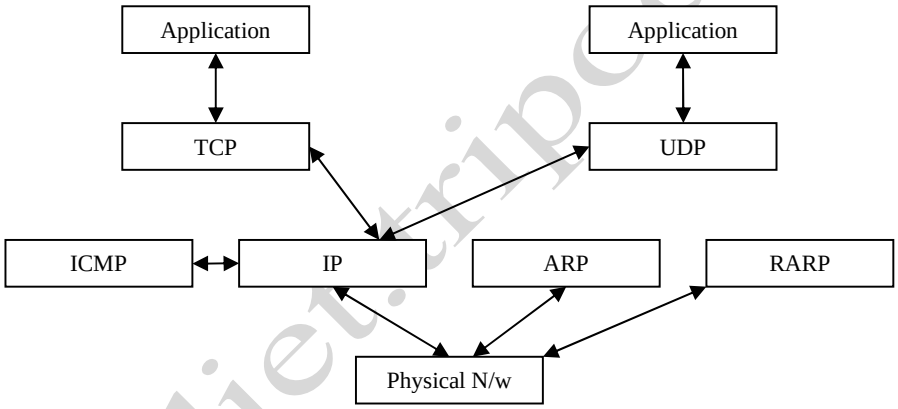


Fig (i)

The PDU of a given layer below as shown in fig (ii). In fig an HTTP request is passed to the TCP Layer, which encapsulates the message into a TCP segment. The segment header contains the port No. for the client process the TCP segment in turn is passed to the IP layer where it is encapsulated in an IP Packet. The IP Packet header contains an IP N/w address for the sender & an IP N/w address for the destination. IP N/w address are said to be logical because they are defined in terms of the logical topology of the routers & end systems. The IP packet is then passed through the N/w interface & encapsulated into a PDU of the underlying N/w in fig (ii)

The IP packet is encapsulated in an Ethernet LAN frame header. The frame header contains physical addresses that identify the physical end points for the sender & the receiver. The logical IP addresses need to be converted into specific physical addresses to carry out the transfer of bits from one device to another. This conversion is done by an ARP (Address Resolution Protocol).

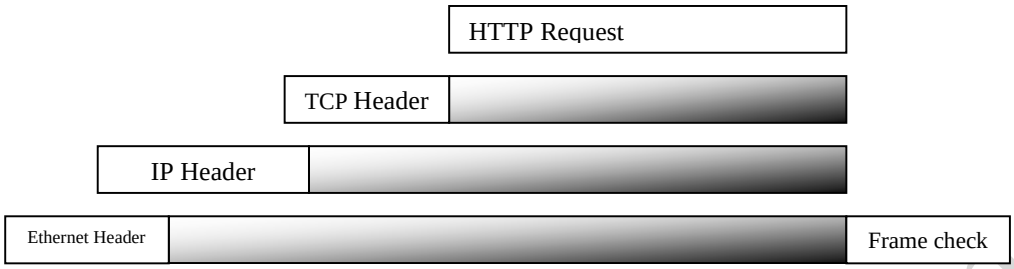


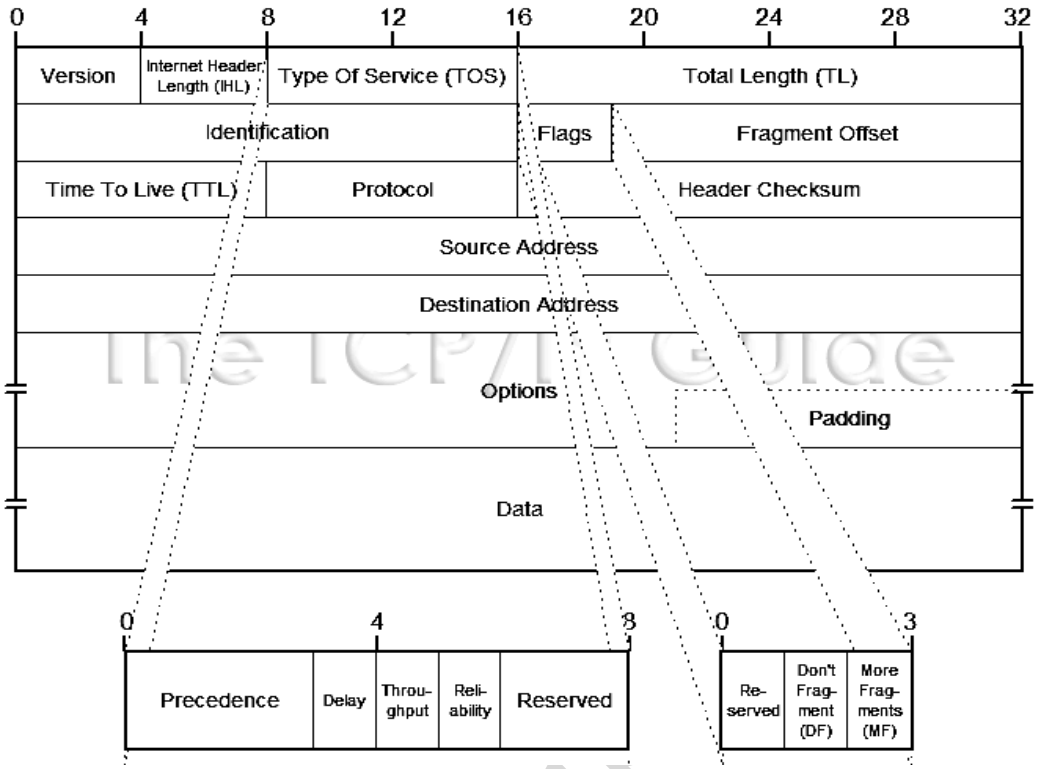
Fig (ii) Encapsulation of PDU's in TCP/IP & addressing information in the headers

The Internet Protocol (IP)

The IP is the heart of the TCP/IP suite. IP corresponds to the N/w layer in the OSI model & provide a connectionless & best-effort delivery service to the transport layer. The term best-effort indicates that IP will try its best to foreword packets to the destination but does not guarantee that a packet will be delivered to the destination.

IP Packet

To understand the services provided by the IP, it is useful to examine the IP Packet format which contains a header part & a data part. The format of IP Header is shown in fig (iii). The Header can be from 20-40 bytes & contain information essential t



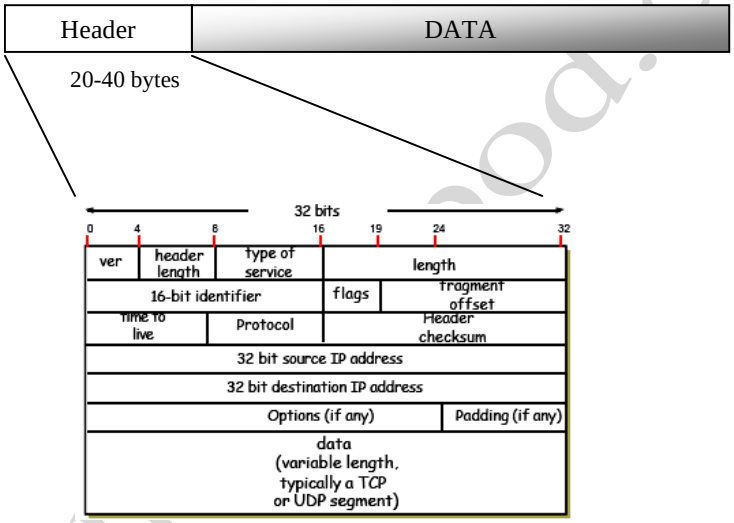
Its various parts are:-

1. **Version (VER):** The first field defines the version no. of the IP addresses. The current version is 4 (IPV4) with a binary value of 0100
2. **Header Length (HLEN):** the HLEN field defines the length of the header in multiples of 4 bytes.
3. **Service Type:** This field specifies the priority of the packet based on the delay, through output, reliability & cost requirement.
4. **Total length:** The total length specifies the no. of bytes the IP Packet including header & data. It is a 16 bit field & can defined upto 65,535 bytes.
5. **Identification:** This field is used in fragmentation, a packet when passing through different networks, may be divided into fragments to match the N/w frame size when this happens each fragment is identified with a sequence number in this field.
6. **Flags:** The bits in the flag field deal with fragmentation i.e. the packet can or can't be fragmented, can be the first, middle or last fragment etc.
7. **Fragmentation Offset:** The fragmentation offset is a pointer that shows the offset of the data in the original packet (If it is fragmented).
8. **Time To Live:** This field is defined to indicate the amount of time in second; the packet is allowed to remain in the N/w. The source host, when creates the packet, set this field to an initial value. As the packet travel through the internet, router by router, each router decrements this value by 1. If this value

becomes 0 before the packet reaches to its final destination, the packet is discarded.

9. **Protocol:** This field defines which upper layer protocol data are encapsulated in the datagram (Ex...TCP,UDP,ICMP)
10. **Header Checksum:** This field verifies the integrity of the header of the IP Packet. The data part is not verified & is left to upper layer protocols. If the verification process fails, the packet is simply discarded.
11. **Source IP & Destination IP Address:** These are four byte (32 bit) field gives the address of the original source & the final destination respectively.
12. **Option:** This field gives more functionality to IP Packet. It can carry fields that control routing, timing, management & alignment & some security level.

FIG (iii)



IP Routing

IP Layer routes the packets from IP N/w sources to destinations. The IP Layer in each host & router maintains a routing table that it uses to determine how to handle each IP packet. If the routing table indicates that the destination host is directly connected to the originating host by a link or by a LAN then the IP Packet is sent directly to the destination. Otherwise, the routing table specifies that the packet is to be sent to a default router that is directly connected to the originating host

When a router receives an IP packet, the router examines its routing table too see whether the packet is destinies to itself, if so delivers the packet to the appropriate higher layer protocol. Each row in the routing must provide the following information:

i. Destination IP Address.
ii. IP address of next hop router.

iii. Several flags, fields & outgoing interface.

Each time a packet is to be routed, the routing table is searched in the following order:

i. The first column is searched to see whether the table contains an entry for the complete destination IP address. If so, then the IP Packet is forwarded according to that to destination.
ii. If the table does not contain the complete destination IP address, then the routing table is searched for the destination N/w ID. If an entry is found the IP Packet is forwarded to that N/w.
iii. If the table does not contain the destination N/w ID the table is searched for a default router entry, & if one available the packet is forwarded there.
iv. If none of above searches are successful, then the packet is declared undeliverable & "Host unreachable error" massage is sent back to the originating host.

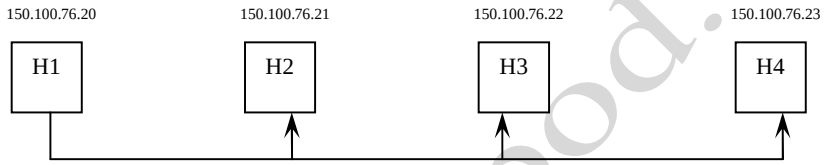
CIDR (Classless Inter-Domain Routing)

Dividing the IP Address space into A, B, & C classes turned out to be inflexible Most Organizations utilize class B address space inefficiently, on the other hand most organisations typically need more addresses than can be provided by a class C address space. Giving class B address space to each organisation would have exhausted the IP address space easily because the rapid growth of the internet.
The class-full address space restriction was lifted. An arbitrary prefix length to indicate the N/w, known as CIDR, it was adopted in place of the class-full scheme. Using a CIDR notation, a prefix 205.100.0.0/22. The corresponding prefix range runs from 205.100.0.0 through 205.100.3.0. The /22 indicates that the N/w mask is 22 bits or 255.255.252.0
CIDR routes the packet according to the higher order bits of the IP address & a 32 bit mask, uses a technique called super-netting so that a single routing entry covers a block of class-full addresses. For e.g. Instead of having 4 entries for a continuous set of class C addresses (0.0, 1.0, 2.0, 3.0, & 4.0)

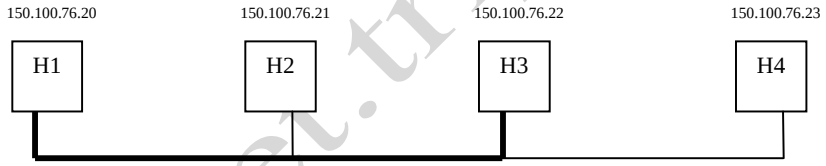
Address Resolution Protocol (ARP):

We assume that a host can send a packet to the destination IP Address. The IP Packets must be delivered by the underlying N/w technology, which uses a different address format. Let us assume the technology is Ethernet. The Ethernet hardware can understand only its own 48 bit MAC addresses (Media Access Control

Address). Format, so the source host must know the destination MAC Address if the packet is to be delivered to the destination.
Now the host has to map the IP address to the MAC address. One solution to find out the destination MAC address is to use the ARP.
Ex is shown in fig. Suppose H1 wants to send an IP Packet to H3 but does not know the MAC Address of H3. H1 First broadcast an ARP Request packet asking the destination host. Destination host is identified by the IP address send by the H1 (source). All hosts in the N/w receive the packet, but only the intended host, which is H3, responds to H1.
The ARP response packet contains H3's MAC & IP address Now H1 Can send packet to H3 avoid having to send an ARP Request packet each time it wants to send a packet to H3, H1 store H3's IP & MAC address in its ARP table. So H1 can look up H3's MAC Address in table for future use.



ARP Request (What is the MAC address of 150.100.76.22?)



ARP Response (My MAC address is 08-00-5A-C5-38-94)

FIG (iv)

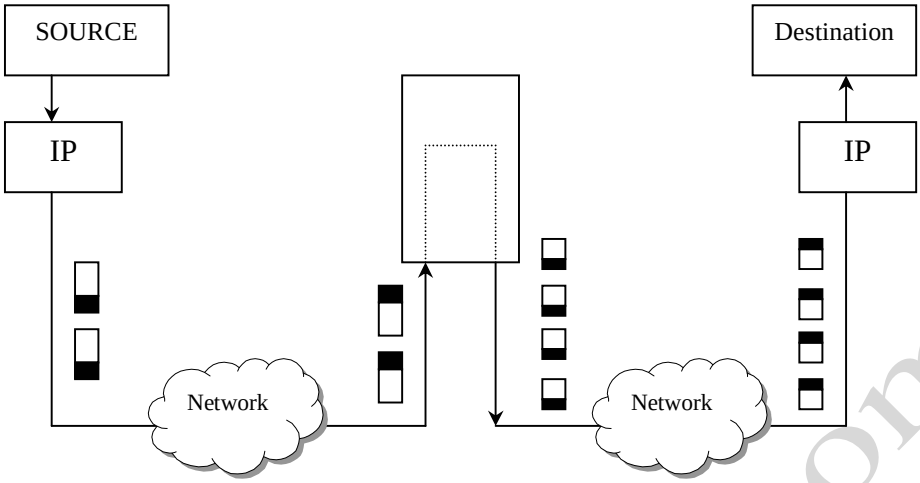
Reverse address resolution protocol (RARP):

Now the host knows the destination MAC address but not the IP address. So the problem of getting an IP address from a MAC address can be handled by RARP.
To obtain the IP address the host first broadcast an RARP request Packet containing its MAC address on the N/w. All hosts receive the packet but whose MAC address match with request packet replies to the host by sending an RARP response packet containing the MAC & IP addresses one limitation with RARP is that the server must be located on the same physical N/w as the host.

Fragmentation & Reassembly:

One of the strength of the IP is that it can work on variety of physical N/w; each physical N/w has pa packet size limitation on the packets that can be carried called the Maximum transmission Unit (MTU). When IP has to send a packet which is larger than the MTU of the physical N/w, IP must break the packet into smaller fragments whose size can be larger than the MTU. Each fragment is sent independently to the destination. If the MTU of some other N/w downstream is found to be smaller than the fragment size then again the fragments are broken into smaller size as shown in the figure.
The destination IP is the only entity that is responsible for reassembling the fragment into the original packet. To reassemble the fragments the destination waits until it has received all the fragments belonging to the same packet. If one or more fragments are lost in the N/w the destination stop the reassembly process & discards the rest of the fragments. To detect the lost fragments, the destination host set a timer. If the timer expires before all the fragments have been received, the host assume the missing fragments were lost in the N/w & discards the other fragments.

Three fields in IP header (Identification, Flag & fragment offset) have been assigned to manage the fragmentation & reassembly. At the destination IP has to collect fragments for reassembly into packets. The identification field is used to identify which packet a particular fragment belongs to so that fragments for different packets do not get mixed up.
The flag field has three bits; one unused bit, one don't fragment bit (DF), one more fragment bit (MF). If DF=1 It forces the router not to fragment the packet. If DF=0 then fragments the packet. If the packet length is greater than the MTU the router will have to discard the packet & send an error message to source host.
The MF bits tell the destination host whether or not more fragments follow. If need more fragments then MF is set to 1 otherwise 0.
The fragment offset field identifies the location of a fragment in a packet.
If one of the fragments is lost the packet can't be reassembled at the destination & rest of the fragments has to be discarded. This process wastes the transmission bandwidth. If the upper layer protocol requires reliability, then all the fragments for that packet would have to be retransmitted.

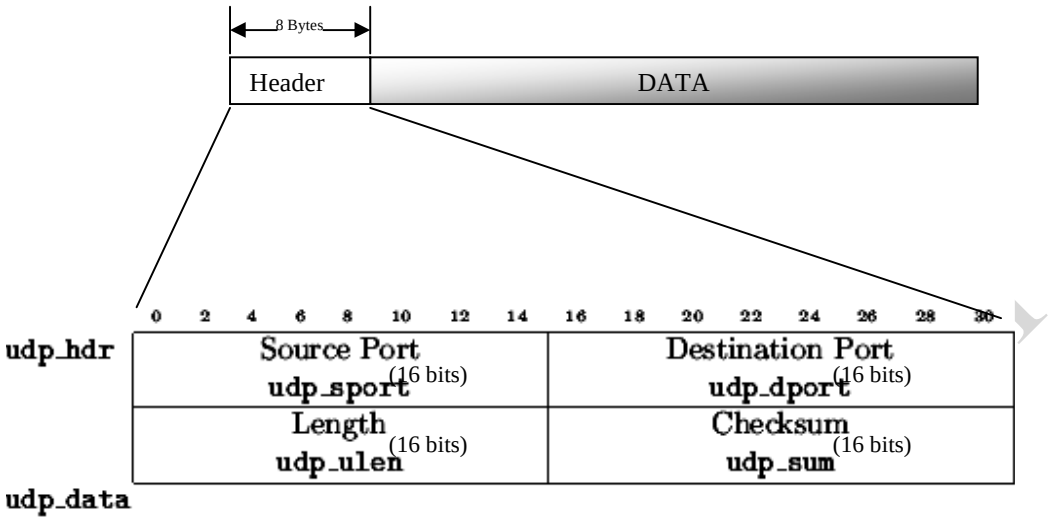


ICMP (Internet Control Message Protocol)

It is a mechanism used by the router if it could not forward a packet for some reasons then it would have to send an error message back to report the problem. The protocol that handles error & control messages is called ICMP.
The IP is an unreliable & connectionless protocol ICMP allows IP to inform a sender if a packet is undeliverable. A packet travels from router to router, until it reaches one that deliver to final destination. If a router is unable to route or deliver the packet because of unusual conditions or because of N/w congestion. ICMP allows it to inform the original source.
ICMP uses echo test/reply to test whether a destination is reachable & responding. It also handles both control & error messages, but its main function is to report about the problems, not to correct them. Responsibility for correction lies with the sender.
A packet carries only the address of the original sender & the final destination. It doesn't know the addresses of the previous router(s) that passed it along. For this reason ICMP can send messages only to source, about the problem not to an intermediate router.

UDP (User Datagram Protocol)

UDP is an unreliable, connectionless transport layer protocol. It is a very simple protocol that provides only two additional services beyond IP : Demultiplexing & error checking on data. Applications that use include TFTP, DNS, SNMP & RTP. The packet produced by UDP is called datagram. The format of UDP datagram is shown in fig (v)



The UDP datagram has following parts:

1. **Source Prot Address:** it is the address of the application program that has created the message. It is a 16 bit field.
2. **Destination Port address:** it is also a 16 bit field. It is the address of the application program that will receive the message & allows the UDP module to demultiplex datagram to correct application in a given host.
3. **Total length:** It defines the total length of the user datagram in bytes (including header & Data).
4. **Check sum:** It is a 16 bit field. It is used to detect the errors in the datagram. If a source doesn't want to compute, this field should contain all 0's.

UDP is a connectionless & unreliable protocol so it doesn't provide any sequencing or recording functions & can't specify the damage packet when reporting an error. UDP can discover that an error has occurred; ICMP can inform the sender that a datagram has been damaged & discarded. Neither, has the ability to specify which packet has been lost. UDP contain only a checksum, it doesn't contain an ID or sequencing Number for a particular data_segment.