Unit 5
Network and Transport Layers

Introduction

The transport and network layers are so closely tied together that they are almost always discussed together. TCP/IP is the most commonly used set of transport and network layer protocols, so this chapter focuses exclusively on TCP/IP.

The transport layer links the application software in the application layer with the network and is responsible for the end-to-end delivery of the message. The transport layer accepts outgoing messages from the application layer (e.g., Web, email, and so on, as described in Chapter 2) and segments them for transmission. The Protocol Data Unit (PDU) at the transport layer is called a **segment.**

The network layer takes the messages from the transport layer and routes them through the network by selecting the best path from computer to computer through the network (and adds an IP packet). The data link layer adds an Ethernet frame and instructs the physical layer hardware when to transmit. As we saw in Chapter 1, each layer in the network has its own set of protocols that are used to hold the data generated by higher layers.

The network and transport layers also accept incoming messages from the data link layer and organize them into coherent messages that are passed to the application layer. For example, as in Figure below a large email message might require several data link layer frames to transmit. The transport layer at the sender would break the message into several smaller segments and give them to the network layer to route, which in turn gives them to the data link layer to transmit. The network layer at the receiver would receive the individual packets from the data link layer, process them, and pass them to the transport layer, which would reassemble them into the one email message before giving it to the application layer.

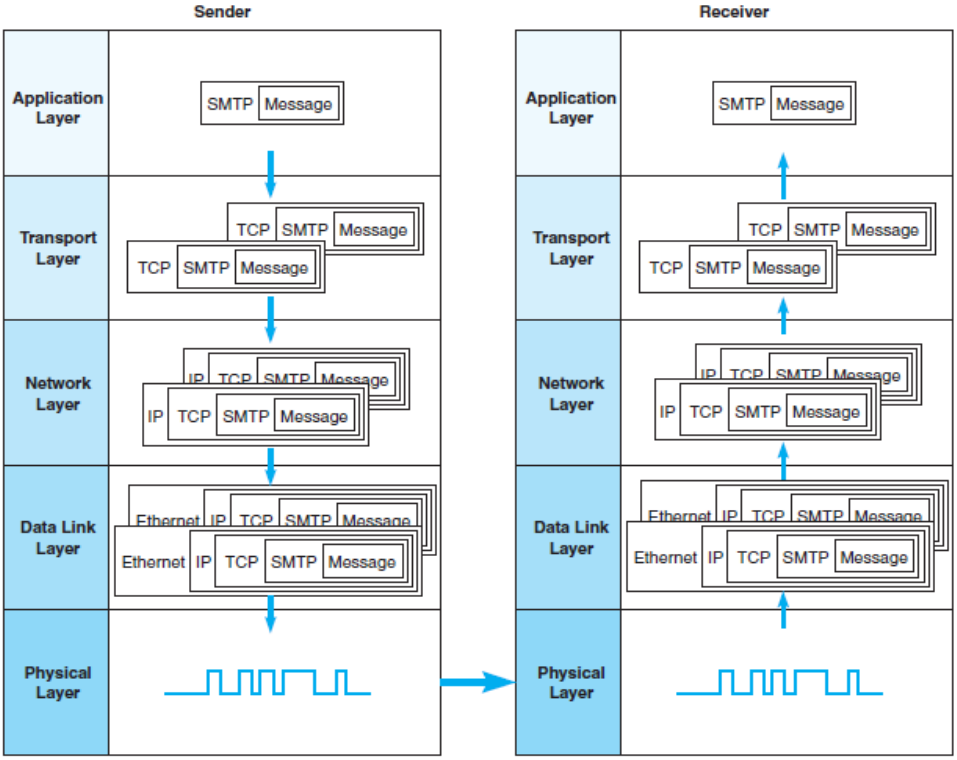


Fig: Message transmission using layers.

Transport and Network Layer Protocols

There are different transport/network layer protocols; however the three main protocols are more focused: **TCP, UDP and IP.**

Transmission Control Protocol (TCP)

TCP is a reliable connection oriented protocol that allows a byte stream originating in one machine to be delivered without error to any other machine. It is said to be connection oriented as before one application process can begin to send data to another. The two processes must handshake with each other (i.e. they must send some preliminary segments to each other to establish the parameters of data transfer). TCP was specifically designed to provide a reliable end to end byte stream overran unreliable internetwork and also to be robust in case of any kinds of failure, TCP has ability to handle flow control and sequencing.

Characteristics

i. **Reliability**: TCP assigns a sequence no. to each byte transmitted and expects a positive acknowledgement from receiving TCP layer. If ACK isn't received within a timeout interval, the data is retransmitted.

ii. **Stream Data Transfer:** TCP transfer a contiguous (continuous) stream of bytes through the network. The application doesn't have to brother with chopping the data into basic blocks or datagram. TCP does this by grouping the bytes into **TCP segments** which are paused to IP layer for transmission to destination.

iii. **Flow Control:** TCP uses sliding window mechanism for implementing the flow control. The receiving TCP when sending an ACK back to sender also indicates to the sender the number of byte it can receive.

iv. **Connection oriented:** TCP establishes a connection before any data transfer. The connections are made between the port numbers of the sender and the receiver devices a **TCP connections** identifies the end points involved in the connection. A **socket number** is a combination of **IP addresses** and **port number**, which can uniquely identify the **connections.**

v. **Full Duplex:** TCP provides for concurrent data streams in both directions.

TCP Segment Format

TCP segment consists of data bytes to be sent and a header that s added to the data by TCP as shown in figure below:

The header of a TCP segment can range from 20-60 bytes. Header fields are:

1. **Source Port Address:** It is 16-bit field that holds the port address of the application that is sending the data.
2. **Destination Port Address:** It is 16-bit field that holds the port address of the application in the host that is receiving the data segment.
3. **Sequence Number:** It is a 32-bit field that holds the sequence number, i.e. the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end if the segments are received out of order.
4. **Acknowledgement Number:** It is a 32-bit field that holds the acknowledgement number, i.e. the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.
5. **Header Length (HLEN):** This is a 4-bit field that indicates the length of the TCP header by number of 4-byte words in the header, i.e. if the header is 20 bytes (min length of TCP

header), then this field will hold 5 (as 5*4=20) and the maximum header length 60 bytes, then it holds the value 15 (15*4=60). The value of this field is between 5 and 15.

6. **Control Flags (Reserved):** There are 6 different 1-bit control bits. Their function is:
   i. **ACK:** This bit field is used to indicate that the value carried in acknowledgement field is valid i.e. the segment contains an acknowledgement for a segment that has been successfully received.
   ii. **URG (Urgent):** The URG bit is used to indicate that there is a data in this segment that the sending side has marked as urgent.
   iii. **PSH (Push Function):** It asks to pass the (buffer) data to upper layer immediately.
   iv. **RST (Reset the Connection):** It reset the connection.
   v. **SYN (Synchronized sequence Number):** Only the first packet send from each end should have this flag set.
   vi. **FIN (Finish):** No more data from sender. It tears down the connection.
7. **Window Size:** This field tells the window size of the sending TCP in bytes.
8. **Checksum:** This field holds the checksum for error detection. It is mandatory in TCP as opposed to UDP.
9. **Urgent Pointer:** This field is used to point to data that is urgently required that needs to reach the receiving process at the earliest. Also location of last byte of the urgent data is shown by urgent pointer so that the interrupted data stream can continue.
10. **Options:** This field gives the options to enhance the TCP protocols by introducing new features according to need. Some TCP options are: Maximum segment size, time-stamps, End of option list

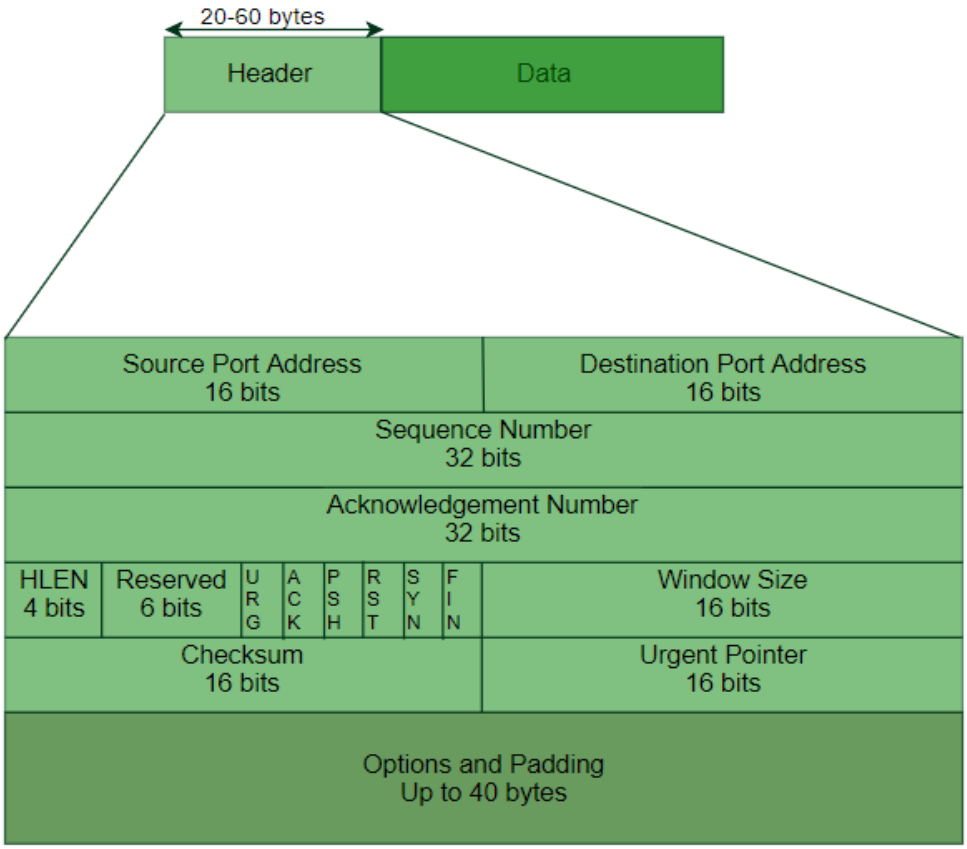


Fig: TCP Segment Header format

Operation of TCP protocol can be divided into 3 distinct sections:

1. **Establishment of Connection**
2. **Data Transfer**
3. **Connection Termination**

1. Establishment of Connection

TCP Connection Using Three –way Handshaking

TCP connection mechanisms works on the following basis:

1. Step 1 (**SYN**): In the first step, clients wants to establish a connection with server, so it sends a segment **SYN (Synchronize Sequence Number)** which informs server that client is likely to start communication and with what sequence number it starts segments with.
2. Step 2 (**SYN+ACK**): Server responds to the client request with **SYN-ACK** signal bits set. Acknowledgement (**ACK**) signifies the response of segment it received and **SYN** signifies with what sequence number it is likely to start the segments with.
3. Step 3 (**ACK**): In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start actual data transfer.

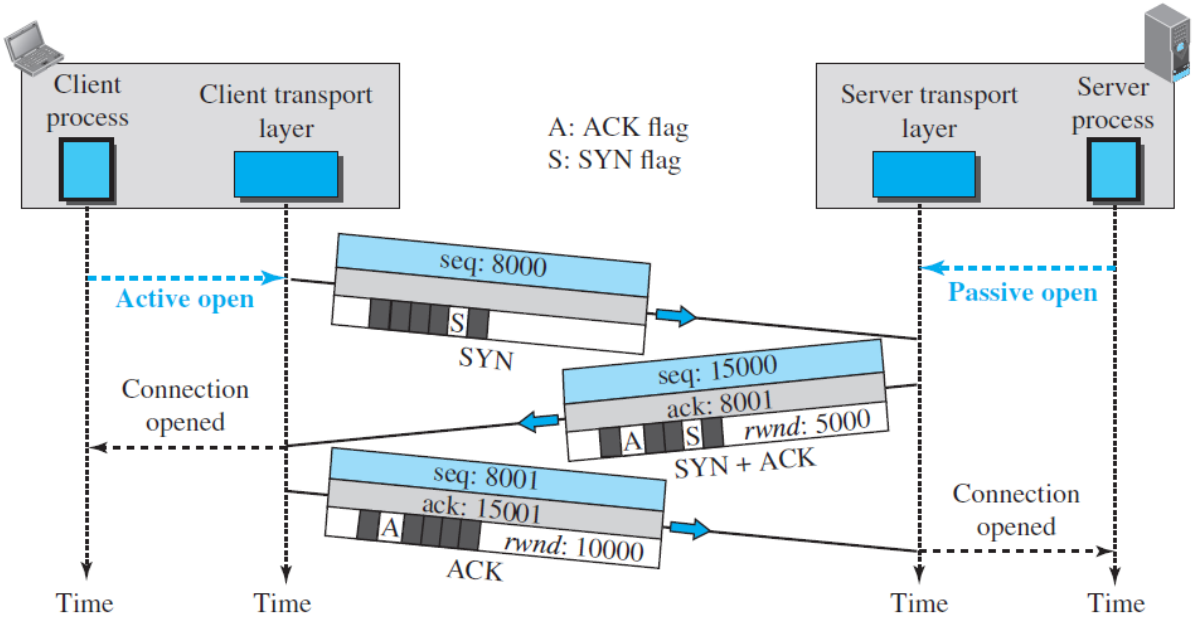


Fig: Connection establishment using three-way handshaking

2. Data Transfer

Data are buffered by transport entity on both transmission and reception. TCP normally exercises its own discretion as to when to construct a segment for transmission and reception. TCP normally exercises in its own discretion as to when to construct a segment for transmission and when to release received data to the user. The **PUSH** flag is used to force the data so far accumulated to be sent by the transmitter and passed on by the receiver. This serves an end-of-block function. The user may specify a block of data as urgent. TCP will designate the end of that block with an urgent pointer and send it out in the ordinary data stream. The receiving user is alerted that urgent data are being received. If during data exchange, a segment arrives that is apparently not meant for the current connection, the RST flag is set on an outgoing segment. Examples of this situation are delayed duplicate SYNs and an acknowledgement of data not yet sent.

3. Connection Termination

Any of two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by client. Most application uses two options for connection termination: **three-way handshaking** and **four-way handshaking.** Most implementations today allow three way handshaking for connection termination as shown in figure below:

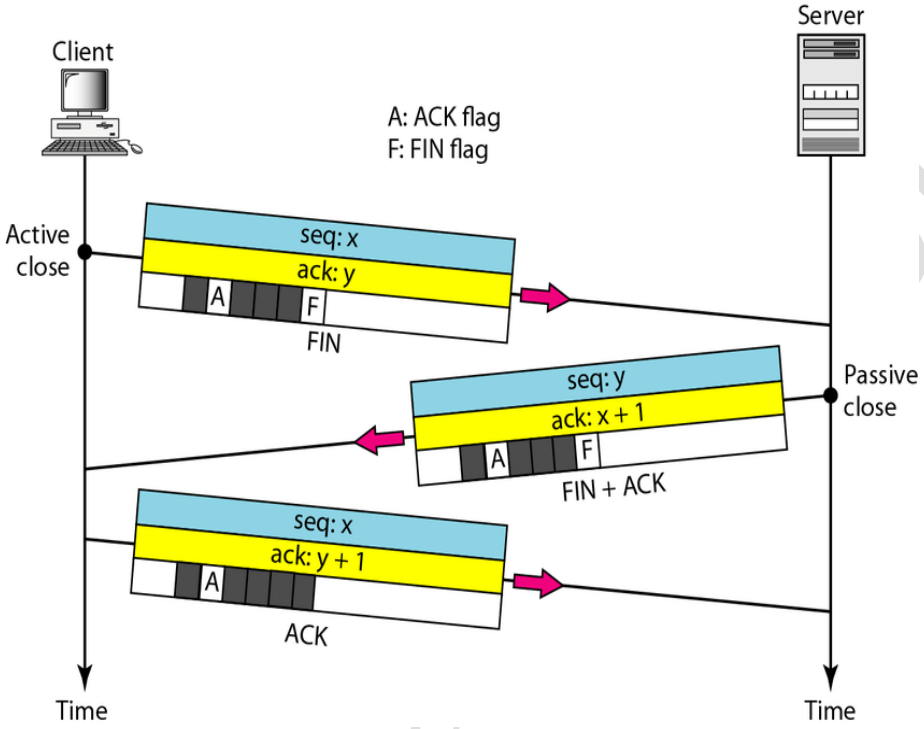


Fig: Connection Termination using three way handshaking

User Datagram Protocol (UDP)

UDP is an alternative communication protocol to TCP used primarily for establishing low-latency and loss-tolerating connections between applications on the internet.

It provide a way application to send encapsulated IP datagram and send them without having to establish a connection. It is useful for applications that don't require or want sequencing, error and flow control. It is especially used for one-shot request, reply application where quick delivery is important. One area where UDP is essentially useful is client server application where client send the short request to the server and expect a quick short reply.

DNS is an application layer protocol that uses UDP. UDP minimizes the overhead associated with message transfer and make communication faster as no network connection is established before transmission.

Features / Characteristics of UDP

i. Connection-less

UDP is a connection less protocol which doesn't require establishing a connection before sending data. UDP just transfer datagram without any formal preliminaries required. So, it doesn't include delay to establish a connection UDP also doesn't maintain connection state and doesn't have receive and send buffers, congestion control parameters, sequencing and ACK number parameter. Because of this, a server devoted to a particular application can typically support many more active clients.

ii. Message / packet oriented

UDP provide a message oriented interface where each packet is send as single UDP segment.

iii. Best effort delivery

UDP offers best effort delivery as IP. This means that the sent segment may be lost, duplicated, corrupted and deliver out of order to application. Because of this feature, UDP is suitable for applications such as voice and video that can tolerate some delivery errors.

iv. Small packet header overhead

Compared to 20-60 bytes of header in TCP segment UDP has only 8 bytes of overhead.

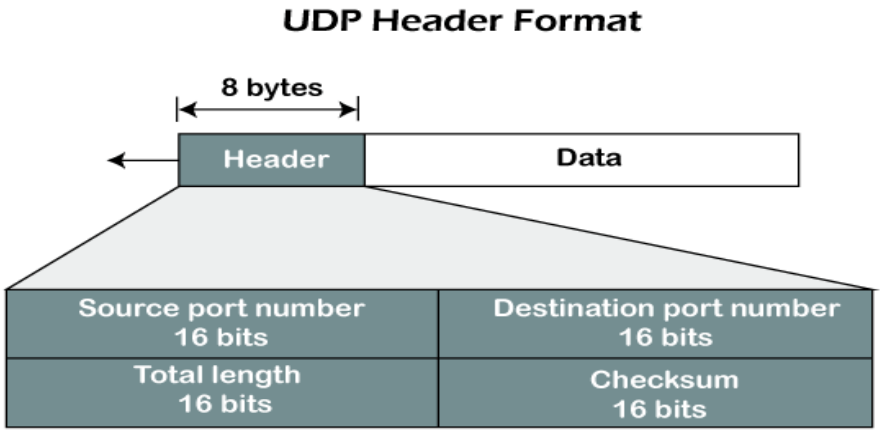


Fig: User Datagram Header Format

1. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
2. **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
3. **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
4. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Internet Protocol (IP)

The **Internet Protocol (IP)** is the host to host N/w layer delivery protocol of Internet. It is unreliable, best effort and connectionless packet delivery protocol. IP use only error detection mechanism & discard the packet if it is corrupted. It does its best to delivery but there is no guarantee. If reliability is important IP is paired with a reliable protocol such as TCP.

IP is also a connection less protocol for packet switching n/w that uses datagram approach i.e. each datagram can follow different route to destination and arrive out of order. There corruption can occur during transition. IP depend on higher level protocol to take care of all these problems.

There are two versions of IP:

1. **IP Version 4 (IPv4)**
2. **IP Version 6 (IPv6)**

IPv4

IPv4 was the primary version brought into action for production within the ARPANET in 1983. IP version four addresses are 32-bit integers which will be expressed in decimal

notation.
Example- 192.0.2.126 could be an IPv4 address.

IPv4 Datagram Format (IPv4 Header Format)

Packets in the network (internet) layer are called datagram. A datagram is a variable length packet consisting of two parts: **header and data.** The header is 20 to 60 bytes in length and contains information essential to routing and delivery. The figure below shows IP datagram format:

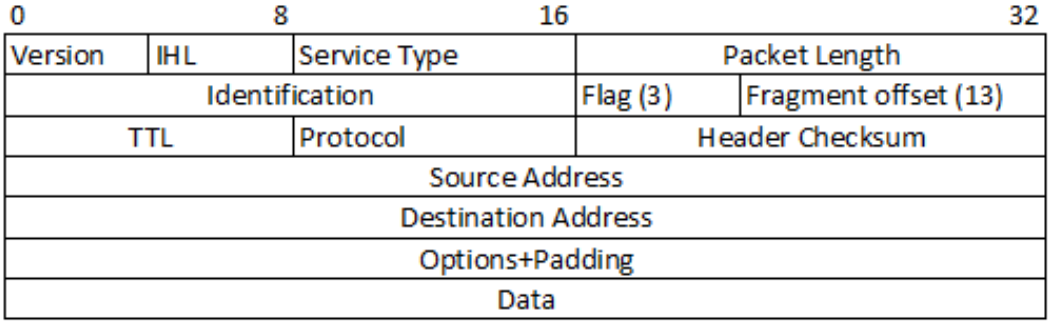


Fig: Header format of IPv4 datagram

1. **Version of IP: Version** of IP address used. It is of 4 bit length.
2. **IHL (Internet Header Length)/header Length (HLEN):** It is of 4 bits. These 4 bits are used to determine where in the IP datagram the data actually begins.
3. **Types of service:** It is of 8 bits. This 8 bit field is used to describe level of service such as delay, through-put or reliability that router should use in processing.
4. **Packet Length**: Packet length is total length IP datagram (header + data). It is 16 bits long. The theoretical maximum size of IP datagram is 65,535 bytes. However, datagram are rarely larger than 1,500 bytes.
5. **Identification (16 bits):** It is a sequence number used to reassemble fragment into packet. It contains an integer that identifies the current datagram fragment.
6. **Flag:** IP Packet (datagram) is too large to handle, the **flag** tells if the packet can be fragmented or not. It consists of 3 bit field of which the two low order bit controls fragmentation. i.e. **The first bit is reserved** (not used**), the second bit** is called **the do not fragment bit.** If its value is 1, the machine must not fragment the datagram. If datagram cannot be passed through any available physical network, it discards the datagram and sends ICMP error message to the host. If the value is 0, the datagram can be fragmented if necessary. The **third bit** is called **the more fragment bit.** If its value is 1, it means the datagram is not the last fragment. If its value is 0, it means this is the last or only fragment.
7. **Fragment off set:** This tells where is in the current datagram this fragment belong as a router may have to fragment a packet when forwarding it from one medium to another that has smaller MTU (Maximum Transmission Unit).
8. **TTL (Time to Live)**: It is a counter used to limit packet life line (maximum hops) a packet can take before it is considered on deliverable.TTL value tells the network how many router (hops) the packet can cross.
9. **Protocol:** The protocol field tells what to do with packet or which layer protocol receives incoming packet after IP processing. For example, a value 6 indicates that the data portion is passed to TCP, while a value 17 indicates that the data is passed to UDP.

10. **Header Checksum:** It helps to ensure IP header integrity as some header field change. Header checksum is useful for detecting error in header.
11. **Source Address:** It is 32-bit field which specifies the address of the Sender (Source) of the packet.
12. **Destination Address:** This 32-bit field specifies the address of the Receiver (Destination) of the packet.
13. **Options**: It allows IP to support various options such as **security, record route, and time stamp**.
14. **Padding**: It is used to ensure header ends on 32 bit boundary
15. **Data (Payload):** in most circumstances, the data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

Example: An IP packet has arrived with the first 8 bits as (**01000010**)$_2$. The receiver discards the packet, why?
There is an error in the packet. The 4 left-most bits (0100) show the version, which is correct. The next bits (0010) show the wrong header length (2*4=8). The minimum number of bytes in the header must be 20. The packet has been corrupted in the transmission.

Example: In an IP packet, the value of HLEN is $(1000)_2$ in binary. How many bytes of options are being carried out by this packet?
The HLEN value is 8, which means the total number of bytes in the header is 8*4 or 32 bytes. The first 20 bytes are the base header and the next 12 bytes re the options.

IPv6 Datagram Format (IPv6 Header Format)
IPV6 address is 4 times larger than IPv4 but the header of an IPv6 is only 2 times larger than that of IPv4. IPv6 headers have one fixed header and zero or more Optional (Extension) Headers. IPv6 datagram packet header has three parts, i.e.

1. **IPv6 datagram packet header (Fixed header)**: All the **necessary information that is essential for router** is kept in the **Fixed Header**.
2. **Extension Header:** The **Extension Header** contains **optional information that helps routers to understand how to handle packet/flow**. IPv6 header points the first extension header; it again points the next extension header if present and so on.
3. **Upper Layer Protocol Data: IPv6** datagram packet extension header points the upper layer protocol header. It can be TCP or UDP or ICMP.

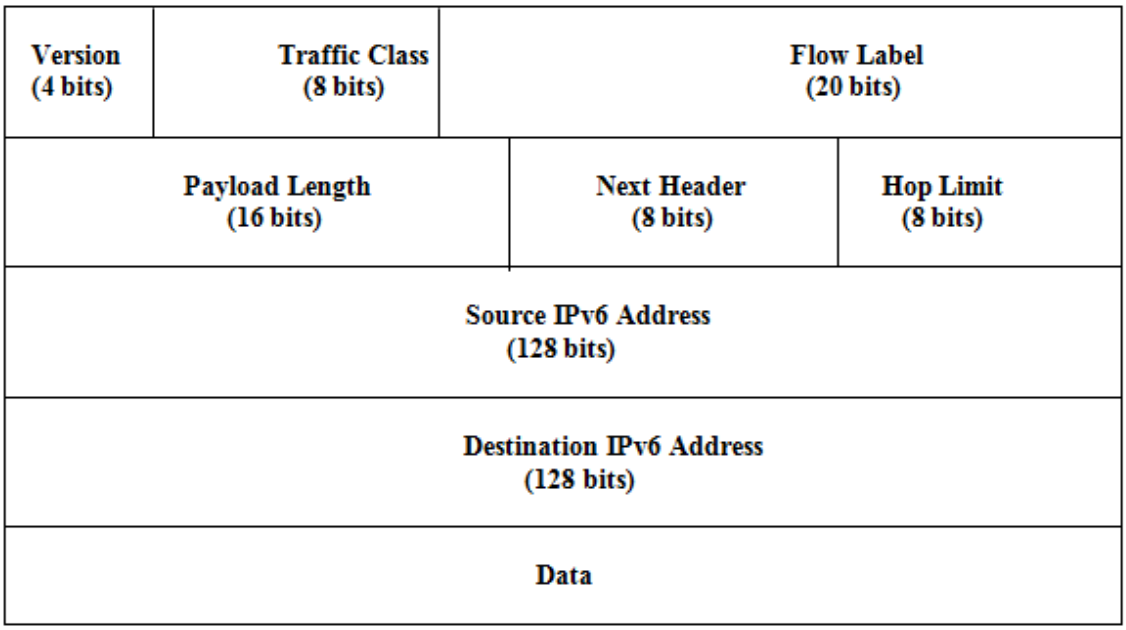


Fig: IPv6 Header Format

1. **Version (4-bits):**4 bit field which identifies the IP's version number.
2. **Traffic Class (8-bits):** the 8 bits are divided into two parts. Most Significant 6 Bits are used for Type of Services to let the router know what services should be provided to this packet. The Least Significant 2 bits are used for **Explicit Congestion Notification (ECN)**
3. **Flow Label (20-bits):** it is used to maintain the sequential flow of packets belonging to a communication.
4. **Payload Length (16-bits):** This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Header and Upper Layer data.
5. **Next Header (8- bits):** This field identifies the protocol to which the contents (data field) of this datagram will be delivered (for example, to TCP, UDP). The field uses the same values as the protocol field in the IPv4 header.
6. **Hop Limit (8-bits):** This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value hop Limit field is decremented by 1 as it passes a link (router/hop). When this field value reaches 0, the packet is discarded.
7. **Source Address (128-bits):** This field indicates the address of originator of the packet.
8. **Destination Address (128-bits):** This field provides the address of intended recipient of the packet.
9. **Data:** This is the payload portion of the IPv6 datagram.

IPv4 to IPv6 Transition Mechanisms

The methods used when transitioning a network from IPv4 to IPv6 are:

1. **Dual Stack:** Running both IPv4 and IPv6 on the same devices.
2. **Tunneling:** Transporting IPv6 traffic through IPv4 network transparently.
3. **Translation:** Converting IPv6 traffic to IPv4 traffic for transport and vice versa.

Transport Layer Functions

1. Linking to the Application Layer (Addressing)

Most computers have many application layer software packages running at the same time. Users often have Web browsers, email programs, and word processors in use at the same time on their client computers. When the transport layer receives an incoming message, the transport layer must decide to which application program it should be delivered. It makes no sense to send a Web page request to email server software. With TCP/IP, each application layer software package has a unique **port address.**

Any message sent to a computer must tell TCP (the transport layer software) the application layer port address that is to receive the message. Therefore, when an application layer program generates an outgoing message, it tells the TCP software its own port address (i.e., the **source port address**) and the port address at the destination computer (i.e., the **destination port address**). These two port addresses are placed in the first two fields in the TCP header segment of above figure (**Fig: TCP Segment Header format**).

Port addresses can be any 16-bit (2-byte) number. Anyone using a Web server should set up the Web server with a port address of 80 and is called the well-known port. Web browsers, therefore, automatically generate a port address of 80 for any Web page clicked. FTP servers use port 21, Telnet 23, SMTP 25, and so on. Network managers are free to use whatever port addresses they want, but if they use a nonstandard port number, then the application layer software on the client must specify the correct port number.

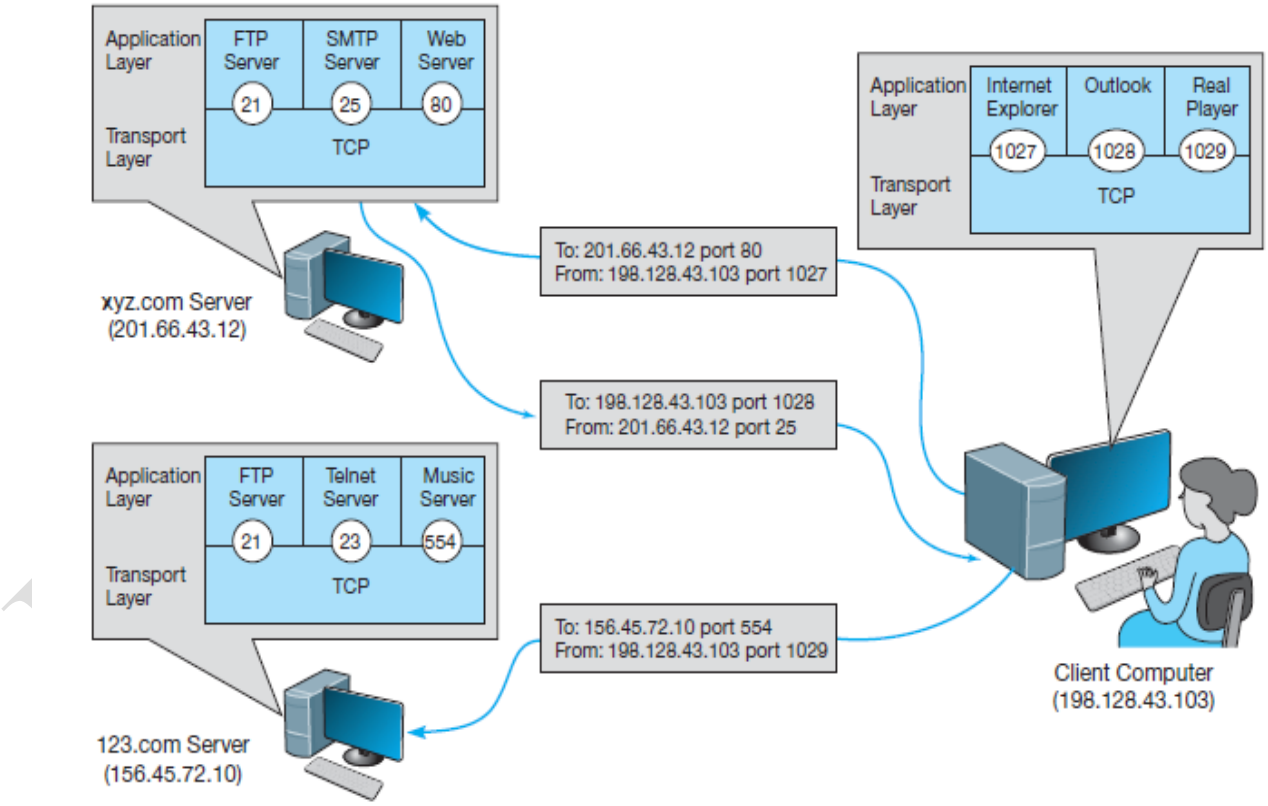


Fig: Linking to application layer services

2. Segmenting

Some messages or blocks of application data are small enough that they can be transmitted in one frame at the data link layer. However, in other cases, the application data in one "message" is too large and must be broken into several frames.

Segmenting means to take one outgoing message from the application layer and break it into a set of smaller segments for transmission through the network. It also means to take the incoming set of smaller segments from the network layer and reassemble them into one message for the application layer. Depending on what the application layer software chooses, the incoming packets can either be delivered one at a time or held until all packets have arrived and the message is complete. The TCP is also responsible for ensuring that the receiver has actually received all segments that have been sent. TCP therefore uses continuous ARQ.

3. Session Management

A **session** can be thought of as a conversation between two computers. When the sending computer wants to send a message to the receiver, it usually starts by establishing a session with that computer. The sender transmits the segments in sequence until the conversation is done, and then the sender ends the session. This approach to session management is called **connection-oriented** messaging. **Connection-oriented messaging** sets up a **TCP connection** (also called a session) between the sender and receiver.

Sometimes, the sender only wants to send one short information message or a request. In this case, the sender may choose not to start a session, but just send the one quick message and move on. This approach is called **connectionless messaging.** When **connectionless messaging** is desired, the TCP segment is replaced with a **User Datagram Protocol (UDP) packet**. The UDP packet is much smaller than the TCP packet (only 8 bytes).Connectionless is most commonly used when the application data or message can fit into one single message.

All of the application layer software we have discussed so far uses TCP i.e. HTTP, SMTP, FTP, Telnet.

UDP is most commonly used for control messages such as addressing DHCP (Dynamic Host Configuration Protocol), routing control messages RIP (Routing Information Protocol) and network management SNMP (Simple Network Management Protocol)

4. Quality of Service

Quality of Service (QoS) routing is a special type of connection-oriented messaging in which different connections are assigned different priorities. For example, videoconferencing requires fast delivery of packets to ensure that the images and voices appear smooth and continuous; they are very time dependent because delays in routing seriously affect the quality of the service provided. Email packets, on the other hand, have no such requirements. Although everyone would like to receive email as fast as possible, a 10-second delay in transmitting an email message does not have the same consequences as a 10-second delay in a videoconferencing packet. With QoS routing, different **classes of service** are defined, each with different priorities. For example, a packet of videoconferencing images would likely get higher priority than would an SMTP packet with an email message and thus be routed first.

5. Congestion control

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur. Again retransmission of packets from the sources increases the congestion further. Transport layer provides Congestion

Control in different ways. It uses **open loop** congestion control to prevent congestion and **closed loop** congestion control to remove the congestion in the network.

6. **Multiplexing and De-multiplexing**

Transport layer provides **multiplexing** mechanism which enable to send packet streams from various applications simultaneously over a network. Transport layer accept these packets from different processes differentiated by their port numbers and passes to network layer. **Demultiplexing** is required at the receiver side to obtain the data coming from various processes. Transport layer receives the segments of data from network layer and delivers it to the appropriate process.

7. **Flow Control:** Transport layer provides end to end flow control
8. **Error Control**

Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error correction is done through retransmission.

Addressing

Any communication that involves two parties needs two addresses: i.e. source address and destination address. However it is extremely important to understand that each computer has several addresses, each used by a different layer. One address is used by the data link layer (MAC/Physical Address) another by the network layer (IP/Logical Address),another by transport Layer (Port Address) and still another by the application layer (Specific Address)

Address	Example Software	Example Address
Application layer	Web browser	www.kelley.indiana.edu
Network layer	Internet Protocol	129.79.127.4
Data link layer	Ethernet	00-0C-00-F5-03-5A

Fig: Types of Addresses

Assigning Addresses

The data link layer address is permanently encoded in each network card, which is why the data link layer address is also commonly called the **physical address** or the **MAC address.** This address is part of the hardware (e.g., Ethernet card) and can never be changed. Hardware manufacturers have an agreement that assigns each manufacturer a unique set of permitted addresses, so even if you buy hardware from different companies, they will never have the same address. Whenever you install a network card into a computer, it immediately has its own data link layer address that uniquely identifies it from every other computer in the world.

At the network-layer the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of device to the Internet. The address associated with network layer is called IP address. Network layer addresses are generally assigned by software. Every network layer software package usually has a configuration file that specifies the network layer address for that computer. Network managers can assign any network layer addresses they want.

It is important to ensure that every computer on the same network has a unique network layer address so that every network has a standards group that defines what network layer addresses can be used by each organization.

At, the transport layer, addresses are called port numbers. Port numbers are local addresses that distinguish between several programs running at the same time.

At the application layer, we normally use names to define the site that provides services, such as facebook.com. Application layer addresses (or server names) are also assigned by a software configuration file. As with network layer addresses, network managers can assign any application layer address they want, but a network standards group must approve application layer addresses to ensure that no two computers have the same application layer address. Network layer addresses and application layer addresses go hand in hand, so the same standards group usually assigns both, e.g., www.indiana.edu at the application layer means 129.79.78.4 at the network layer.

IPv4 Addressing

IP address is 32 bit number represented in a dotted decimal format i.e. as a decimal representation in of four 8 bit values concatenated with dots. A 32-bit address contains two primary parts: **network number/prefix and the host number.** All hosts within a single network share the same network address. Each host has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique. Devices that are visible to users outside the network (e.g. web servers) must have a globally unique IP address. Devices that are visible within the network must have locally unique IP address.

IP addresses are assigned by a central numbering authority called the **Internet Assigned Number Authority (IANA).**

E.g. **128.2.7.9**

N/w Number = 128.2 **Host Number =** 7.9

In binary form: 10000000. 00000010. 00000111. 00001001.

Note:

An IP address identifies an interface that is capable of sending and receiving IP datagram. If a host is on two networks, it must have two IP address. Thus, IP address does not refer to a host.

Rules for IP address

1. All Network IDs cannot be zero.
2. All host IDs can't be one.

- **Default Network:** The IP address **0.0.0.0** is used as default N/w address.
- **Loop back Address:** The IP address **127.0.0.1** is used for loop back address. This means that it is used by host computer to send the message back to itself. It is basically used for troubleshooting and n/w testing.
- **Broadcast Address:** Message that is intended for all computers in an N/W are sent as broadcast. This message always use IP address **255.255.255.255**

IPv4 Classful Addressing/ Class Based IP Address

The first bit of IP address specifies how the rest of address should be separated into N/w & host part. Each address class specifies a different number of bits for its network number/prefix and host number. Classful address is no longer used but a reference to it in literature is still common (classless IP is used). There are 5 classes of IP address.

1. Class A

This address use 7 bits for N/w & 24 bits for host portion of IP address. This allows 2^7 **128** N/Ws each with $2^{24} - 2 = 16777214$ hosts.

Class A address has a network number in between 0 to 127 as its first part. Host number within class A is represented by any combination of numbers in the next three parts. Class A contains millions of host number in the next three parts. Class A contains millions of host number and is generally used by large organization.

Class A ranges from 0 to 127 but 127.X.X.X is reserved for loop back address. The actual address of class A is 0 to 126.

The ranges for class A IP address is:

Minimum value	**00000001**	**1**	**000000**	**1.H.H.H**	**1.H.H.H**
Maximum value	**01111111**	**127**	**0111111.H.H.H**	**127.H.H.H**	

Subnet mask of class A= 255.0.0.0

E.g.: 127.8.9.2

2. Class B

This address use 14 bits for N/W & 16 bits for host portion. This allows 2^{14} **=16384** possible N/Ws each with $2^{16}-2$ **= 65534** hosts.

A class B IP address has 128 to 191 in its first part. In 4 parts of IP address the first two parts represent the N/W and last two parts represent the host. Each N/W has more than 64000 host address. Class B is generally used by medium size of the organization.

The ranges for class B IP address is:

Minimum value	**10000000**	**128**	**10000000.N.H.H**	**128.N.H.H**
Maximum value	**10111111**	**191**	**10111111.N.H.H**	**191.N.H.H**

Subnet Mask of Class B = 255.255.0.0

E.g.: 128.2.7.9

3. Class C

This address use 22 bits for N/W & 8 bits for host portion. This allows 2^{21} **= 2097152** possible N/Ws each with 2^8 **-2 = 254** hosts.

A class C IP address begins with the number in between 192 to 223 in its first part. In 4 parts the first three parts of an IP address represent the N/W and only the last part represent a specific host. This class is basically used by small sized business organization.

The ranges for class C IP address is:

Minimum value	**11000000**	**192**	**11000000.N.N.H**	**192.N.N.H**
Maximum value	**11011111**	**223**	**11011111.N.N.H**	**223.N.N.H**

Subnet Mask of Class C = 255.255.255.0

E.g.: 192.168.1.3

4. Class D

This address are reserved for multicasting (a sort of broadcasting but in a limited area and only to host using same class D address.) e.g. Video Configuration

Ranges from 224.0.0.0 to 239.255.255.255

5. Class E

Class E is used for future use, research purpose. It ranges from 240.0.0.0 to 254.255.255.254.

Pictorial representation of IP Classes

8	16	24	32		
0 Network	Host	Host	Host	**A**	**0.0.0.0 to 127.255.255.255**
10 Network	Network	Host	Host	**B**	**128.0.0.0 to 191.255.255.255**
110 Network	Network	Network	Host	**C**	**192.0.0.0 to 223.255.255.255**
1110	Multicast Address			**D**	**224.0.0.0 to 239.255.255.255**
1111	Reserved for future use & research			**E**	**240.0.0.0 to 254.255.255.255**

Note: While calculating host IP address 2 IP addresses are decreased because they cannot be assigned to hosts. The first IP of a network is N/W number and last IP is reserved for Broadcast IP.

Network Mask /Subnet Mask

The network mask/subnet mask is used for separating the network part and host part of any IP address. 1's in a subnet mask defines a network part and 0's define host part.

The default subnet mask of Class A, Class B, & Class C IP address are:

IP Address Default	**Subnet Mask**
Class A	**255.0.0.0**
Class B	**255.255.0.0**
Class C	**255.255.255.0**

These IP addresses that use the default IP subnet mask are called **classful IP Address** and those IP addresses that does not use default subnet mask are called **classless IP address.**

Subnet

Subnet is a segment of large IP network that derives its network address from a single standard network address. Sub-netting is the process of breaking down the main classes' i.e. A, B, C network into subnets.

A subnet mask is used to define which bits of an **IP Address make network portion and host portion**. A subnet mask is a same basic thing as a net mask with only the real difference being that you are breaking a large organization network into smaller parts and each smaller section will use a different set of IP address.

When setting up subnet, the following must be determined:

- Number of segment (sub-network)
- Host per segment (how many host per each network)

Advantage of Sub-networking

i. **Network Traffic Isolation:** Less traffic on each subnet
ii. **Simplify administration:** Network may be managed independently
iii. **Improve Security:** Subnet can isolate internal networks so they aren't visible from external network.

Some Important points of subnet

- **Network ID:** First address of subnet is called Network Id
- **Broadcast ID:** There are two types of broadcast.
  - **Direct Broadcast or Local Broadcast:** It is the last address of subnet and can be hear by all hosts in subnet.
  - **Full Broadcast:** It is the last address of IP classes and can be hear by all IP hosts in a network. Full broadcast address is **255.255.255.255.**
- **Host Addresses:** All addresses between the network address (N/W ID) and direct broadcast (Local Broadcast) is called host address for the subnet.
- **Block Size:** Block size is the size of subnet including N/W address, host addresses and broadcast address.

Numerical Examples of different Classes

Q. Suppose you are network administrator of ABC organization which uses N/w Addresses 220.221.222.0 which need to separate among five different departments. Now obtain a subnet mask, N/w address, broadcast address and usable host of every subnet.

We have practiced in class. Numericals are available in your copy.

Some more examples required.

Classless Inter-domain Routing (CIDR)

CIDR is asset of standard that is used to create unique identification for network and host. After the introduction of CIDR, the technique to identify the network and host part is easier. The notation system was developed to make the process more efficient and standard.

CIDR is a slash (/) notation of subnet mask. CIDR tells number of on bits in a n/w address.

- Class A has default subnet mask 255.0.0.0 that means first octet of the subnet mask has all on bits. In slash notation it would be written as /8, means address has 8 bits on.
- Class B has default subnet mask 255.255.0.0 that means first two octet of the subnet mask has all on bits. In slash notation it would be written as /16, means address has 16 bits on.
- Class c has default subnet mask 255.255.255.0 that means first three octet of the subnet mask has all on bits. In slash notation it would be written as /24, means address has 24 bits on.

CIDR IP address consists of two group, network part and host part. In contrast to classful routing which categorize address into one of three blocks, CIDR allows for a block of IP address to be allocated for an internet service provider. Some other examples are:

100.0.0.0/27
192.0.0.0/12
178.0.0.0/10

Numerical Examples of CIDR are available in your copy. We have practiced it in class.

VLSM (Variable Length Subnet Mask)

The problem with fixed length subnet mask is that it generates all of the subnet having equal number of the usable host but all the departments might not have equal number of the host practically. This might create the possibility of large number of the IP wastage.

VLSM is the sub-netting technique that divides the network according to the user's requirement. This creates less wastage of IP. VLSM is also called subnet of sub-netting.

Numerical Examples of VLSM are available in your copy. We have practiced it in class.

Dynamic Addressing

To this point, we have said that every computer knows its network layer address from configuration file that is installed when the computer is first attached to the network. However, this leads to the major network management problem. Any time a computer is moved or its network is assigned a new address, the software on each individual computer must be updated. This is not difficult, but it is very time consuming. The easiest way around this is **dynamic addressing.** With this approach, a server is designated to supply a network layer address to a computer each time the computer connects to the network. This is commonly done for client computers but usually not done for servers.

The most common standard for dynamic addressing is **Dynamic Host Configuration Protocol (DHCP).**

Dynamic Host Configuration Protocol (DHCP)

It is a client server auto-configuration protocol that allows a host to obtain IP address dynamically. The network administrator needs not to set up an individual profile to each device. DHCP just requires a range of IP address on a DHCP server.

Goal

- Dynamically obtained IP address from the network server without intervention of network admin.
- Allow reuse of IP address (hold when connected)

Processes of DHCP

1. **DHCP discover**

The first task of a newly arriving host is to find the DHCP server with which to interact. A DHCPDISCOVER message is sent by client using a DHCP datagram to port 67. Since client doesn't know servers IP, it broadcast the IP datagram containing DHCP discover message using destination address 255.255.255.255 and host address of 0.0.0.0. The discovery message is received by all. The discovery may have a transaction ID that allows subsequent message/response to be matched to discovery request.

2. **DHCP server offer**

After receiving discover message, the DHCP server respond back to client with a DHCP offer. Since, several DHCP server cab be present in network, client may receive multiple offer. Each server offer message with transaction ID of discover message, purpose for client, network mask and IP lease time.

3. **DHCP request**

The client will choose among one or many server offer and respond to its selected offer with a DHCP request message echoing back the configuration parameters.

4. **DHCP acknowledgement**

The server responds to DHCP request message with a DHCP ACK message confirming the requested parameters.

The components involved in DHCP are:

DHCP server

A server is that dynamically allocate IP address to client machine using DHCP. It is responsible for answering request from client and giving IP address to them. It gives client at least two pieces of the TCP/IP configuration information.

- IP address of client.
- Subnet mask

It can also pass additional setting to client:

- Address of first router of client.
- Name and IP address of DNS server

DHCP Client

A host on a TCP/IP network that get its IP address assigned dynamically using DHCP.

DHCP client reservation

It is a process for configuring a DHCP server so those particular hosts on a network always lease same IP address. Reservation for client is done if we want the server to always assign the same IP address to specific machine in a network. Generally IP is reserved for servers.

DHCP lease period

The duration for which a server loans an IP to a DHCP client is DHCP lease period.

DHCP relay agent

It is used when a DHCP server need to lease IP address information to client on multiple subnets. It make unnecessary to maintain DHCP server in each subnet.

Address Resolution

To send a message, the sender must be able to translate the application layer address (or server name) of the destination into a network layer address (IP Address) and in turn translate

that into a data link layer address (MAC Address). This process is called **address resolution.** There are many different approaches to address resolution.

TCP/IP uses two different approaches, one for resolving application layer addresses into IP addresses and a different one for resolving IP addresses into data link layer addresses.

Server Name Resolution

Server name resolution is the translation of application layer addresses into network layer addresses (e.g., translating an Internet address such as www.yahoo.com into an IP address such as 204.71.200.74). This is done using the **Domain Name Service (DNS).**

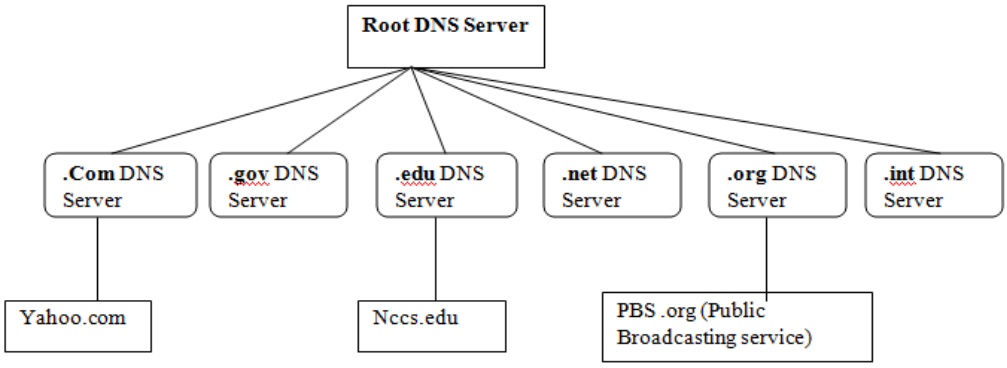
Domain Name Service

It is an internet service that translates domain names into IP addresses. DNS is a hierarchical naming system built on a distributed database implemented in hierarchy of many servers. It is application layer protocol that allows the host, router, name server to communicate to resolve name.

It is said that computer can memorize no. and human can memorize letters. So to provide the compatibility between the two DNS is used. It translates domain name meaningful for human into numerical identifier i.e. to corresponding IP address. For e.g. www.example.com can be translated to 198.105.232.4.

DNS assigns domain names and maps the names to IP addresses by designating an authoritative name server for each domain. These servers are responsible for particular domains and can assign the authoritative name servers to sub-domains. As a result of this process, DNS is both distributed and fault tolerant.

The DNS server uses a large no. of servers organized in a hierarchical fashion and distributed around the world. No single server has all mapping for all host in the internet instead. Mapping is distributed across the DNS server.
Three classes of DNS server are organized in the hierarchy.



1. Root DNS Server
2. Top Level Domain
3. Authoritative DNS Server

How does DNS work?

1. Request information (local cache, it is DNS query)
2. Ask the recursive DNS server- ISP DNS query computer that answers question about the domain name such as IP address,

3. Ask the Top Level Domain name Server: The RLD reviews the next pair of our request (www.google.com).
4. Ask the authoritative DNS server review the next pair of our request and direct our query to the name servers responsible for this specific domain. Authoritative name servers are responsible for knowing all information about a specific domain, which are stored in DNS records.
5. Retrieve the record: check the TTL (Time to Leave) and store the record in its local cache.

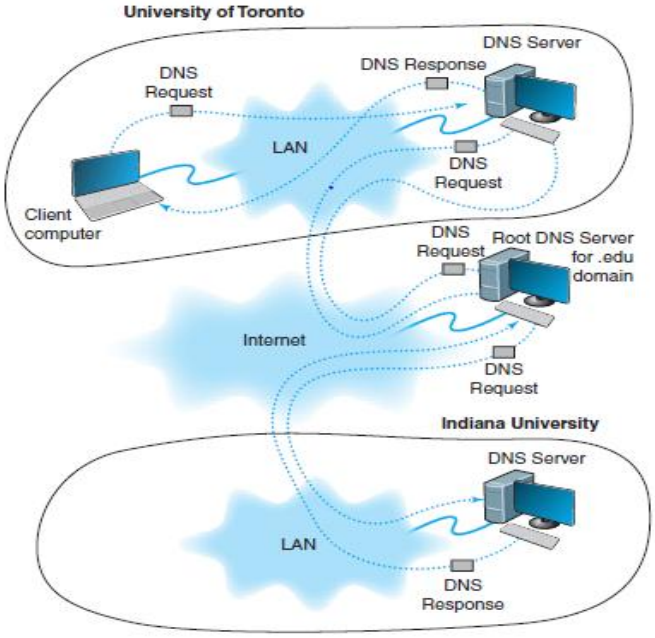


Fig: How DNS work

There are three types of queries in the DNS system

1. **Recursive Query**
2. **Iterative Query**
3. **Non-Recursive Query**

Recursive Query: In a recursive query, a DNS client provides a hostname and the DNS Resolver must provide an answer. It responds with either a relevant resource record or an error message if not found. The resolver starts a recursive query process, starting from the DNS root server, until it finds the Authoritative Name Server that holds the IP address and other information for the requested hostname.

Iterative Query: In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.

Non-Recursive Query: A non recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely

holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

Data Link layer Address Resolution

The **Address Resolution Protocol (ARP**) is a protocol that connects an ever- changing **IP Address** to a fixed physical machine address, also known as **MAC Address,** in a LAN. This mapping procedure is important because the lengths of IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. MAC address is data link layer address which establishes and terminates a connection between two physically connected devices so that transfer can take place. IP address is Network Layer Address and network layer is responsible for forwarding packets of data through different routers. **ARP** works between these layers.

When a computer joins a LAN, it will receive a unique IP address to use for identification and communication. Packets of data arrive at a gateway, destined for a particular host machine. The gateway asks the ARP program to find a MAC address that matches the IP address. There are three basic ARP terms:

1. **Reverse ARP:** It is used is LAN by client machines for requesting IP Address from Router's ARP Table.
2. **Proxy ARP:** It works to enable devices that are separated into network segments connected through the router in the same IP to resolve IP Address to MAC Address.
3. **Inverse ARP:** It uses MAC address to find the IP Address.

Routing

It is the process of selecting paths in a network along which to send N/W traffic. It is to find path between source and destination. It can be defined as a process of forwarding packets from one network to another. Logical addressing is used to identify each network as well as each device on the network.

Routing is a process which is performed by layer 3 (network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

A router makes decision based upon the destination IP address to send the packet in the right direction to reach its destination. To make the correct decision router must learn how to reach remote network.

Information is complied into a routing table which maps the required destination to one or more interface. Routing table is either created manually or by using a dynamic routing protocol and shall be maintained to reflect latest network topology.

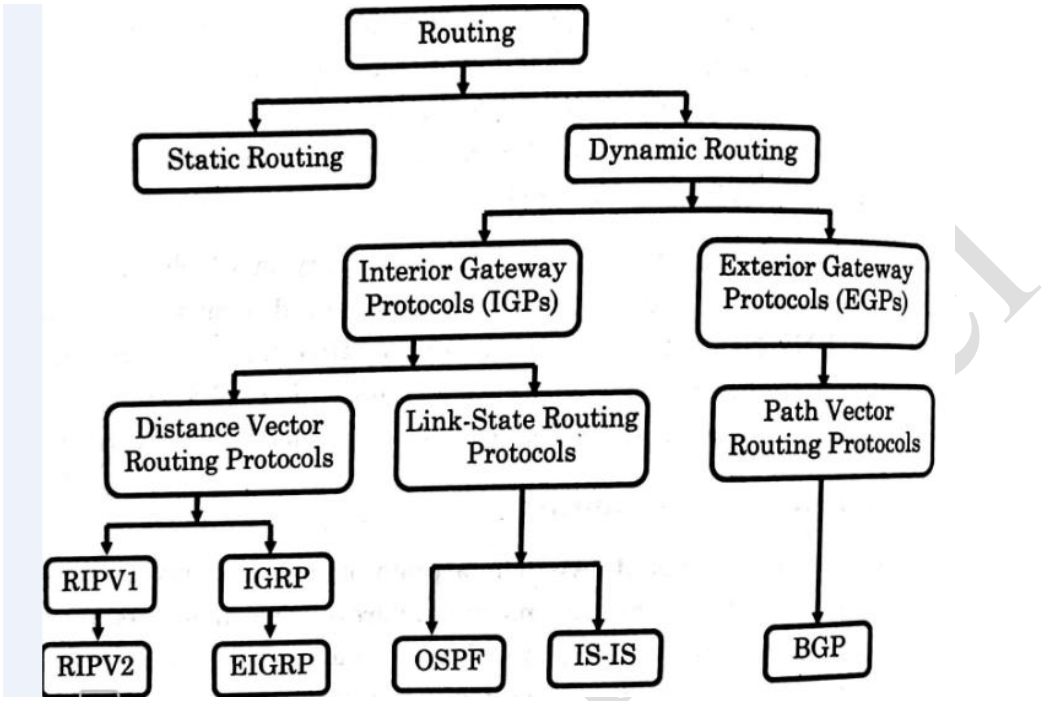
It includes:

1. **Centralized Routing**
2. **Static Routing**
3. **Dynamic Routing**

Centralized Routing

With centralized routing, all routing decisions are made by one central computer or router. Centralized routing is commonly used in host-based networks, and in this case, routing decisions are rather simple. All computers are connected to the central computer, so any message that

needs to be routed is simply sent to the central computer, which in turn retransmits the message on the appropriate circuit to the destination.



Static Routing

Static routing is decentralized, which means that all computers or routers in the network make their own routing decisions following a formal routing protocol. In MANs and WANs, the routing table for each computer is developed by its individual network manager (although network managers often share information). In LANs or backbones, the routing tables used by all computers on the network are usually developed by one individual or a committee.

With static routing, routing decisions are made in a fixed manner by individual computers or routers. The routing table is developed by the network manager, and it changes only when computers are added to or removed from the network. Static routing is commonly used in networks that have few routing options that seldom change.

Advantages

1. Easily implemented in a small network.
2. No overheads are produced on router CPU.
3. Secure because the routes are managed statically.
4. It is predictable as the route to the destination is fixed.
5. Bandwidth usage is not required between routers.

Disadvantages

1. Unsuitable for complex and large networks
2. Large networks increase configuration complexity and time consumption.
3. Link failure can hinder traffic rerouting.
4. The administrator must be extra careful while configuring the routes.

Dynamic Routing

With dynamic routing (or adaptive routing), routing decisions are made in a decentralized manner by individual computers. This approach is used when there are multiple routes through a network, and it is important to select the best route.
Dynamic routing attempts to improve network performance by routing messages over the fastest possible route, away from busy circuits and busy computers. An initial routing table is developed by the network manager but is continuously updated by the computers themselves to reflect changing network conditions.

Advantages

1. Suitable for all topologies.
2. Network size doesn't affect the router operations.
3. Topologies are adapted automatically to reroute the traffic.

Disadvantages

1. Initially it could be complicated to implement.
2. The broadcasting and multicasting of routing updates makes it less secure
3. Routes rely on current topologies.
4. Additional resources are required such as CPU, memory and link bandwidth.

Dynamic Routing includes:

1. **Distance Vector Dynamic Routing Protocols**
2. **Link state Dynamic Routing Protocols**
3. **Interior Vs Exterior Dynamic Routing**

Distance Vector Dynamic Routing Protocols

Distance vector means that routes are advertised as vectors of distance & direction. This routing algorithm uses Bellman-Ford algorithm. The distance from source to destination is defined in terms of metric such as hop count & direction.

Process/Activities Performed

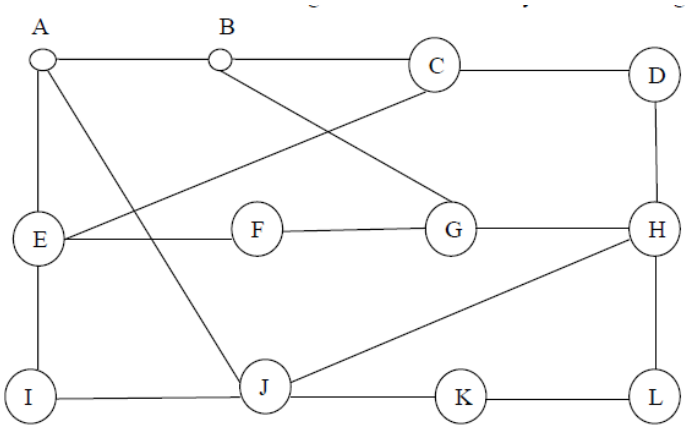
1. Determine the direction & distance to any link on the inter-n/w.
2. It periodically sends all or some portion of the routing table to their adjacent neighbor.
3. Send periodic updates even if there is no change in n/w.
4. Use Bellman-Ford algorithm to find the best path.
5. This algorithm upgrades by having each router maintain a table giving the best known distance to each destination and which line to use to get there.

Table contains:

i. The preferred outgoing line to use for that destination.
ii. Estimate of time or distance to that destination

Working

Each router receives a routing table from its directly connected neighbor router.
In figure below Router B receives information from router A. Router B adds a distance vector number such as number of hops. This number increases the distance vector. Then, router B passes this new routing table to its neighbor 'C'. This same step-by-step process occurs in all directions between neighbor routers.



Examples of Distance Vector Protocol are: **Routing Information Protocol (RIP), Interior Gateway Protocol (IGRP)**

Benefits of Distance Vector Routing

i. Simple to implement
ii. Low memory & CPU requirement
iii. Can be run by cheap router

Problems in distance vector Routing

i. Incomplete view of n/w topology.
ii. Generally updates are periodic and send full routing table.
iii. Class full routing protocol.
iv. Potential for loops in algorithm.

Link state Dynamic Routing Protocols

This algorithm uses the principle of the link state to determine n/w topology.

A link state is the description of an interface on a router (E.g. IP address, subnet mask, type of n/w) and its relationship to neighboring router. The collection of these link state forms a link state database. The process used by link state algorithm to determine n/w topology is straightforward.

The link state algorithm is also known as **shortest path first algorithm**. The link state routing algorithm maintains a complex database of topology information which gives full knowledge of distant router & how they inter-connect. Bandwidth is commonly used to define the state of link and the best link is the link with highest bandwidth or lowest cost between nodes.

The **steps** are:

1. Each router identifies all other routing devices on the directly connected n/w.
2. Each router advertises a list of all directly connected n/w links & the associated cost of each link. This is performed through the exchange of Link State Advertisement (LSA) with other routers in the n/w.
3. Using this advertisement, each router creates a database detailing the current n/w topology. The topology database in each router is identical.
4. Each router uses the information in the topology database to compute the most desirable routes to each destination. This information is used to update the IP routing table.

Advantages /Benefits

1. Quicker convergent
2. Usually better selection of shortest path.
3. Minimal bandwidth used on N/W state change

Problems

1. Memory requirement to store the database is high.
2. CPU requirement to rebuild the tree when a new advertisement arrives is high.

Q. Differentiate between Distance vector Routing and Link State Routing?

Routing Protocols

A routing protocol is a protocol that is used to exchange information among computers to enable them to build and maintain their routing tables. A routing protocol can be considered as the language that is used to build the routing tables.

It can be useful to know all possible routes to a given destination. However, as a network gets quite large, knowing all possible routes become impractical; there are simply too many possible routes. Even at some modest number of computers, dynamic routing protocols become impractical because of the amount of network traffic they generate. For this reason, networks are often subdivided into **autonomous systems** of networks.

An **autonomous system** is simply a network operated by one organization, such as IBM or Indiana University, or an organization that runs one part of the Internet.

Remember that we said the Internet was simply a network of networks. Each part of the Internet is run by a separate organization such as AT&T, MCI, and so on. Each part of the Internet or each large organizational network connected to the Internet can be a separate autonomous system.
The computers within each autonomous system know about the other computers in that system and usually exchange routing information because the number of computers is kept manageable. If an autonomous system grows too large, it can be split into smaller parts. The routing protocols used inside an autonomous system are called **interior routing protocols.** Protocols used between autonomous systems are called **exterior routing protocols.**

Although interior routing protocols are usually designed to provide detailed routing information about all or most computers inside the autonomous systems, exterior protocols are designed to be more careful in the information they provide.. There are many different protocols that are used to exchange routing information.

The commonly used protocol on the Internet are :

1. **Border Gateway Protocol (BGP)**
2. **Internet Control Message Protocol (ICMP)**
3. **Routing Information Protocol (RIP)**
4. **Intermediate System to Intermediate System (IS-IS)**
5. **Open Shortest Path First (OSPF)**
6. **Enhanced Interior Gateway Routing Protocol (EIGRP).**

Border Gateway Protocol (BGP)

It is an inter-autonomous routing protocol used on the edge of an AS. It is the protocol used on the edge of an AS. It is the protocol which is used to make core routing decisions on the internet. It is the path vector protocol or a variant of distance vector routing protocol. It is an exterior routing protocol which is used for the exchange of information in internet and it is used between different ISPs. BGP is very robust and scalable routing protocol. It is considered to use a path vector routing algorithm which means it tracks the path in terms of which autonomous system; it passes through and is not capable of load balancing or packet forwarding itself. Full routing updates are sent at the start session and trigger updates are sent subsequently.

The connection is maintained by periodic “keep alive” message. The failure to see a keep alive an update or notification is the means by which destination networks and path to those destination are tracked. Any change in n/w results a trigger update.

BGP basics are:

1. The current version of BGP is BGP version 4, based on RFC4271.
2. BGP is the path-vector protocol that provides routing information for autonomous system on the Internet via its AS-Path attribute.
3. BGP is a layer 4 protocol that sits on top of TCP. It is much simpler than OSPF, because it doesn't have to worry about the things TCP will handle.
4. Peers that have been manually configured to exchange routing information will form a RCP connection and begin speaking BGP. There is no discovery I BGP.
5. Medium sized businesses usually get into BGP for the purpose of true multi-homing for their entire network.
6. An important aspect of BGP is that the AS-Path itself is an anti-loop mechanism. Routers will not import any routes that contain themselves in the AS-Path.

Internet Control Message Protocol (ICMP)

ICMP is the simplest interior routing protocol on the Internet. ICMP is simply an error-reporting protocol that enables computers to report routing errors to message senders. ICMP also has a very limited ability to update routing tables. ICMP packets include an ICMP header after normal IP header. When a router or server needs to send an error message, the ICMP packet body or data section always contains a copy of the IP header of the packet that caused the error.

There are different types of ICMP messages, such as:

1. **Echo reply (Type 0):** A response to an echo request.
2. **Destination unreachable (Type 3):** The destination is unreachable.
3. **Redirect Message (Type 5):** The datagram should be sent via a different route.
4. **Echo Request (Type 8):** A request to echo the enclosed packet of data.
5. **Time Exceeded (Type 11):** The datagram is discarded because it was not delivered within a certain time frame.
6. **Parameter problem (Type 12):** The datagram has a parameter problem and cannot be processed

ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic distance vector interior routing protocol that is commonly used in smaller networks, such as those operated by one organization.

The network manager uses RIP to develop the routing table. When new computers are added, RIP simply counts the number of computers in the possible routes to the destination and selects the route with the least number. Computers using RIP send broadcast messages every minute or so (the timing is set by the network manager) announcing their routing status to all other computers. RIP is used by both TCP/IP and IPX/SPX.

Intermediate System to Intermediate System (IS-IS)

IS-IS is a link state interior routing protocol that is commonly used in large networks. IS-IS is an ISO protocol that has been added to many TCP/IP networks.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic hybrid interior routing protocol that is commonly used on the Internet. It uses the number of computers in a route as well as network traffic and error rates to select the best route. OSPF is more efficient than RIP because it normally doesn't use broadcast messages. Instead, it selectively sends status update messages directly to selected computers or routers. OSPF is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to Designated Router (DR)/ Backup Designated Router (BDR).

OSPF is the preferred interior routing protocol used by TCP/IP. It is an interior gateway protocol developed by IETF (Internet Engineering Task Force) based on link status. It is used for routing in an

autonomous System. On IP N/w it collects and transfers the link status of Autonomous System to dynamically discover and advertise route. The link status protocol is developed to compensate the limitation and defects of distance vector protocol.

Some terms of OSPF are:

1. **Router I'd**: It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router Priority:** It is an 8 bits value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR):** It is elected to minimize the number of advances formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all other routers share their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR):** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and perform its functions.

Advantages of OSPF

i. **Area Assignment:** OSPF allows the n/w of an AS to be divided into several areas, & logically segment the n/w to decrease the size of routing table;
ii. **Parallel rate:** OSPF supports multiple parallel routers to send destination.
iii. **Support authentication & Encryption:** OSPF supports interface based packet authentication so as to guarantee the security of routers and calculations.
iv. **Multicast Transmission:** OSPF send protocol packet on the link layer with the multicast transmitting capability to the multicast address.
v. It supports various n/w scales and can support almost several 100 routers.
vi. It selects the path according bandwidth.
vii. Fast convergence.
viii. OSPF supports VLSM (Variable Length Subnet Masking) & CIDR (Classless Inter Domain Routing).
ix. OSPF only send updates on routing table instead of whole routing table.

Disadvantages of OSPF

i. In the initial discovery process, the link status routing protocols will flood packets on the n/w transmission line. So the capabilities of the n/w to transmit data will be greatly weakened.
ii. Link status routes are sensitive to storage capacity and processors processing capabilities. OSPF maintains a multiple copies of routing information increasing the amount of memory involved,
iii. Hard to understand the process of this routing algorithm.

Enhanced Interior Gateway Routing Protocol (EIGRP).

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic hybrid interior routing protocol developed by Cisco and is commonly used inside organizations. Hybrid means that it has some features that act like distance vector protocols and some other features that act like link-state protocols. As you might expect, EIGRP is an improved version of **Interior Gateway Routing Protocol (IGRP).** 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.

Multicasting

The most common type of message in a network is the transmission between two computers. One computer sends a message to another computer (e.g., a client requesting a Web page). This is called a **Unicast Message.** Typically, an IP address refers to an individual host on a particular network. IP also accommodates addresses that refer to group of hosts on one or more networks. Such addresses are referred to as **multicast addresses,** and the act of sending a packet from a source to the members of a

multicast group is referred to as **multicasting.** Computers wishing to participate in a multicast send a message to the sending computer or some other computer performing routing along the way using a special type of packet called **Internet Group Management Protocol (IGMP).** Multicasting has number of practical applications. For example,

1. **Multimedia:** A number of users "tune in" to a video or audio transmission from a multimedia source station.
2. **Teleconferencing:** A group of workstations from a multicast group such that a transmission from any member is received by all other group members.
3. **Database:** All copies of a replicated file or database are updated at the same time.
4. **Distributed Computation:** Intermediate results are sent to all participants.
5. **Real-time workgroup:** Files, graphics, and messages are exchanged among active group members in real time.

The Anatomy of a Router
TCP/IP Example

- **Known Addresses,**
- **Unknown Addresses,**
- **TCP Connections**
- **TCP/IP and Network Layers**

Consult book for these Topics