ktunotes.in

GET IT ON Google Play

KTU NOTES

The learning companion.

KTU STUDY MATERIALS | SYLLABUS | LIVE NOTIFICATIONS | SOLVED QUESTION PAPERS

Website: www.ktunotes.in

Module VI

Transport layer & Application layer.

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.

Transport layer ensures that the whole message arrives and provide error control and flow control at the source to destination.

* Transport layer is responsible for the delivery of a message from one process to another

Transport layer provides service to the application layer and takes service from Network layer.

Note:- Node to Node delivery – Data link layer.
host to host delivery – Network layer
process to process delivery – Transport layer

MOUNT ZION COLLEGE OF ENGINEERING
Department of Computer Science & Information Technology
KADAMANNITTA

A transport layer protocol can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

A connection oriented transport layer make a connection with transport layer at the destination machine first before delivering the packets. After all the data is transferred, the connection is terminated.

ENGINEERING
Department of Computer Science & Information Technology
KADAMANNITTA

* The transport level protocol will require an additional address, known as port Number, to select a particular process among multiple processes running on the destination host.

At the transport level, communication can take place between process or application programs by using port address.

* Transport layer address is specified with the help of a 16 bit port number in the range of '0' to 65535

Internet Assigned Number Authority (IANA) has divided the address in three Ranges. 1) well-known ports.
2) Registered ports. 3) Dynamic ports.

DOWNLOADED FROM KTUNOTES.IN

* Well-known ports :- The ports in range from '0' to '1023' are assigned and controlled by IANA. These port numbers are commonly used as universal port number in the server for the convenience of many clients.

* Registered ports :

Registered ports in the range from 1024 to 49151 are not assigned or controlled by IANA. However, they can only be registered with IANA to avoid duplication.

* Dynamic ports :- (Ephemeral port numbers)

Dynamic ports (49152 – 65535) are neither controlled by IANA nor need to be registered. They can be defined at the client site and chosen randomly by the transport layer software.

Well-known ports (UDP) Examples.

port	protocol
7	– Echo.
9	– Discard.
11	– user
13	– ~~Dynamic~~ Daytime
53	– DNS.
67	– BOOTP server.
68	– BOOTP client
69	– TFTP
111	– RPC.
123	– NTP
161	– SNMP

Note : Socket Address

process-to-process delivery need two identifiers, IP address and port number at each end to make connection.

The combination of an IP address and port number is called socket address. The client socket address defines the client process uniquely and server socket address defines the server process uniquely.

TFTP → Trivial File transfer Protocol

RPC → Remote procedure Ca

NTP → Network Time protoco

SNMP → Simple Network Mangen Protocol

Note :-

In the internet, the transport layer address are called port in ATM networks, they are called AAL-SAPs. Generic term is Transport Service Access point (TSAP), then Netwo layer address is called NSAPs (Network service Access point). IP addresses are example of NSAPs.

* Duties of transport layer

1) Packetizing. 2) Connection control
3) Addressing. 4) Providing reliablity

DOWNLOADED FROM KTUNOTES.IN

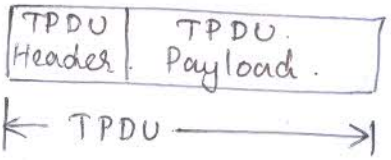
Packetizing :- The transport layer create packet out of the messag received from the application layer. Packetizing is the process of dividing a long message into smaller one. These packets a then encapsulated into the data field of the transport layer packet and headers are added.

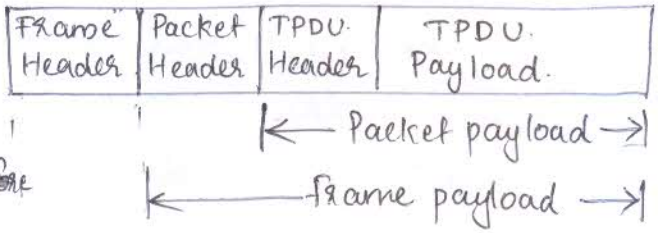
- TPDU (Transport protocol Data unit)

Connection control

Transport layer protocol may be divided into following two categories.

1) connection oriented delivery
2) Connection less delivery.





Addressing

Computer often run several programs at the same time ~~therefore~~ therefore transport layer need to addressing diffrent programs using port number.

Providing reliablity

flow control and error control should be incoporated. Transport layer must provide a reliable packet delivery for process to process.

* Typical QoS parameters for transport layer.

1) Connection establishment delay :- The time difference between the instant at which transport connection is requested and the instant at which it is confirmed is called as connection establishment delay. The shorter the delay the better the service

2) Connection establishment failure probablity :- It is the probabli that connection is not established even after the maximum connec establishment delay. This can be due to network congestion or some other problem.

3) Throughput : It measures the number of bytes of user data transferred per second, measured over some time interva It is measured seperately for each direction.

4) Transit delay :- It is the time for a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine.

DOWNLOADED FROM KTUNOTES.IN

5) Residual error ratio :- It ~~means~~ measures the number of lost messages as a function of total message sent. Ideal the value of this ratio should be zero and practically it should be small as possible.

6) Protection :- This parameter provides a way to protect the transmitted data from being read or modified by some unauthorized parties.

7) Priority :- This parameter provides a way for the user to show that some of its connection (or process) are more important than the other one.

8) Resilence :- Due to internal problem or congestion, the transport layer spontaneously terminates a connection. the resilence parameter gives the probability of such a termination

* Transport Service primitives.

The transport service primitives allow the transport user such as application programs to access the transport service. Each transport service has its own service primitives

Primitive	TDPU Sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	Connection request	Actively attempt to establish a connection
SEND	Data	send data
RECEIVE	(none)	Block until a data TPDU arrives.
DISCONNECT	Disconnection request	Replace the connection

* In order to implement the transport layer services between two two transport entities, ~~what~~ we have to use a transport protocol

-the Transport protocols have to deal with the following tasks. 1) Error control 2) Sequencing 3) Flow control.

Important
* Elements of transport protocols.

1) Addressing - TSAP (Transport Service Access point)
- Socket addressing.

2) Establishing a Connection. - connection established between and destination (process to process)

DOWNLOADED FROM KTUNOTES.IN

3) Releasing a connection – Proper connection release fro both side (close the connection)

4) Flow control & Buffering – for flow control, a sliding window is required on each connection to keep a fast transmitter from overrunning a slow receiv
– the sender should buffer outgoing TPUDs until they are acknowledged
– Receiver accept TPUDs only when a free buffer is availa at receiver side.

5) Multiplexing & Demultiplexing – addressing mechanism allows multiplexing & demultiplexing by t transport layer.

6) Crash recovery – The crash can be recovered by re-tran smitting the lost one.

* The Internet transport protocols (TCP & UDP)

The internet has two main protocols in the transpo layer. One of them is connection oriented and other one support connection less service.

TCP (Transmission control protocol) is a connection oriented protocol and UDP (User's datagram protocol) is a connectionless protocol

* TCP (Transmission Control protocol)

TCP provides a connection-oriented, full duplex, reliable streamed delivery service using IP to transport messages between two processes.

Reliablity is ensured by
* Connection Oriented Service.
* Flow control using sliding window protocol
* Error detection using Checksum
* Error control using go-back-N ARQ technique.
* Congestion avoidance algorithms.

For Obtaining the TCP service, it is necessary for both sender and receiver to create end point called sockets. Each socket has a socket number or socket address.

DOWNLOADED FROM KTUNOTES.IN

The Socket address of two parts
1) IP address.
2) port Numbers.

In order to obtain TCP service, it is necessary to establish a connection between the sockets on the sending and receiving machines.

Socket call		Meaning
Socket	—	Create a new end point (socket)
BIND	—	Give a local address to a socket
LISTEN	—	Show willingness to accept connection
ACCEPT	—	Block the caller until a connection attempt arrives.
CONNECT	—	Attempt to make a connection.
SEND	—	Send the data over the connection.
RECEIVE	—	Receiver data over the connection.
CLOSE	—	Release the connection.

* the same Socket can be used for establishing more than one connection at a time. connections are identified by the socket identifiers at both ends.
* TCP does not support multicasting or broadcasting.
* TCP connection is a byte stream and not a message stream.
* when a application passes data to TCP, the TCP may send it immediately or may collect the data for some time and send at once. (which is called buffering)
* If an application wants the data to be sent immediately, the it can use PUSH flag which will force the TCP to send data without any delay.
* If the sending application puts some control information in the data stream and gives it to TCP along with the URGENT flag then the TCP will stop accumulating data and transmit everything it has for that connection immediately.
ie, URGENT flag is always indicate the urgent data.

TCP services

Services offered by TCP to the processes at the application layer
1) process-to-process communication.

DOWNLOADED FROM KTUNOTES.IN numbers.

2) Stream Delivery Service.

TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.

3) Sending & Receiving Buffer.

The sending and receiving process may not read data at the same speed. TCP needs buffers for storage there are two buffers, the sending buffer and the receiving buffer. One for each direction.

4) Segments.

The Network layer as a service provider for TCP needs to send data in packets. not as stream of bytes. At the transport layer, TCP groups a number of bytes together into a packets called a segments, TCP adds a header to each segment *the segments are encapsulated in IP datagrams.

5) Full duplex Communication

data can flow in both directions at the same time, Each TCP then has a sending and receiving buffe

6) Connection-Oriented Service.

a) the two TCPs establish a connection between them
b) Data are exchanged in both direction.
c) The connection is terminated.

7) Reliable Service.

It use an acknowledgment mechanism to check the safe and sound arrival of data.

TCP Features.

1) Numbering System
   - Byte number
   - Sequence number.
   - Acknowledgment Number.

Byte number : TCP number all data bytes that are transmitted in the numbering starts with a randomly generated number bytes are numbered from 1057 to 7056

Sequence number:- After the bytes have been numbered, TCP assign a sequence number to each segment that have being sent. The sequence number for each segment is carried in the segment.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

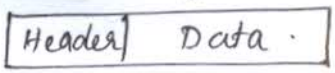
Acknowledgement Number : The value of the acknowledgement field in a segment defines the number of the next byte a receiver expects to receive,
The acknowledgement number is cumulative, means that if a receiver uses 5643 as an acknowledgment number, it has received all bytes from the beginning up to 5642.

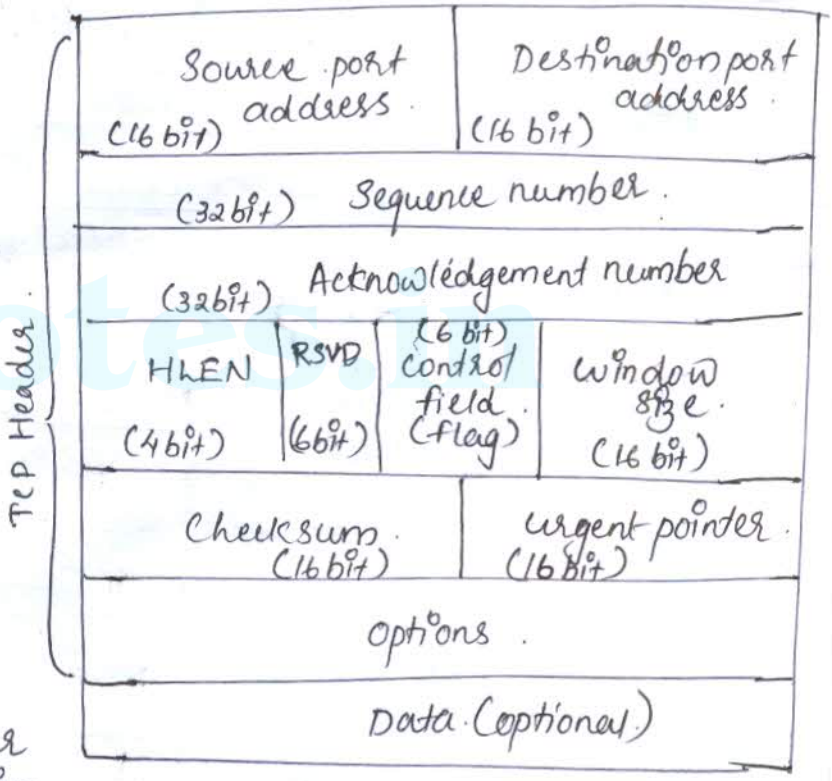
2) Flow control
3) Error control
4) Congestion control

* TCP header format

- The TCP segment consist of a 20-60 byte header.
- The header is 20 bytes if there is no options and up to 60 bytes if it contain options.

TCP Segment





Source port address
- 16 bit field.
- It defines the port number of the application program in the host of the sender.

Destination port address
- 16 bit field.
- It defines the port number of the application program in the host of the receiver.

Sequence number
- 32 bit field, defines the number assigned to the first byte of data contained in this segment.
- During the connection establishment, each party uses a random ~~number~~ number generator to create an Initial sequence number (ISN), which is usually different in each direction.

Acknowledgment number.
- 32 bit field, defines the byte number that the receiver of the segment is expecting to receive from the other party.

DOWNLOADED FROM KTUNOTES.IN

Header length (HLEN)
- 4 bit field, indicate the total header length (length between 20-60byte) ie, value of field can be between 5 (5x4=20) and 15 (15x4=60).

Reserved (RSVD)
- 6 bit field reserved for future use.

Control (Flag)
- 6 diffrent control bits or flags, one or more of these bits can be set at a time.

URG	ACK	PSH	RST	SYN	FIN

← 6 bit control field →

Flag	Description
URG	– The value of urgent pointer field is valid.
ACK	– The value of the acknowledgment field is valid.
PSH	– push the data
RST	– Reset the connection
SYN	– Synchronize sequence numbers during connection
FIN	– Terminate the connection.

Window size
- 16 bit field.
- define the size of window, in bytes that the other party must maintain.
- maximum size of the window is 65,535 bytes.
- normaly the value referred to as the receiving window.

Checksum.
- 16 bit field, contains the checksum of Header (error detection)

Urgent pointer.
- 16 bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.

Options.
- Optional 40 bytes of informations.

* TCP connection
TCP is connection-Oriented, A TCP protocol establishes a virtual path between the source and destination. All the segment belonging to a message are then sent over this virtual path.
- Acknowledgment & re-transmission of damaged or lost frame.
- if a segments arrives out of order, the TCP holds it until the missing segment arrive.

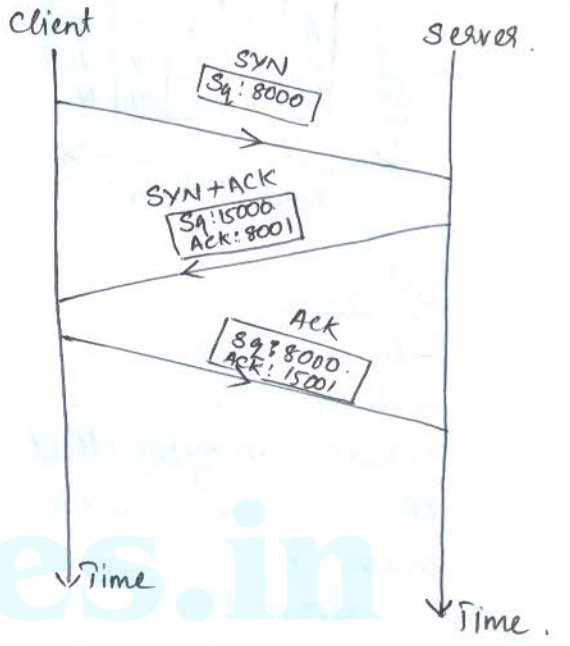
Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

TCP connection-Oriented transmission require three phases.
1) Connection establishment
2) data transfer.
3) Connection termination.

Connection establishment
- TCP transmit data in full duplex mode.
- Each party must initialize communication and get approval from the other party before any data are transferred.

* The connection establishment in TCP is called Three-way Handshaking



Step① The client sends the first segment, a 'SYN' segment, in which only the SYN flag is set. This segment is for synchronization of sequence number, it consume one sequence number. When data transfer starts, the sequence number is incremented by 1
- A SYN segment cannot carry data, but it consume one sequence number.

Step② The server sends the second segment, a SYN+ACK segment, with 2 flag bit set. SYN & ACK. This segment has a dual purpose.
- SYN for communication in the other direction.
- Ack for the acknowledgment of client SYN segment.
- A SYN+ACK segment cannot carry data, but does consume one sequence number of server and acknowledgement number.

Step③ The client sent the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment (or first segment sent by server)
- An ACK segment, if carry no data, consume no sequence number.

* This 3 steps show how TCP connection establishment ~~take place~~ occure.

Data transfer
After connection establishment, bidirectional data transfer can take place the client and server can send data and acknowledgments.
- The data segments sent by the client have the PSH (Push) flag set so that the server TCP knows to deliver data to the server process as soon as they received.

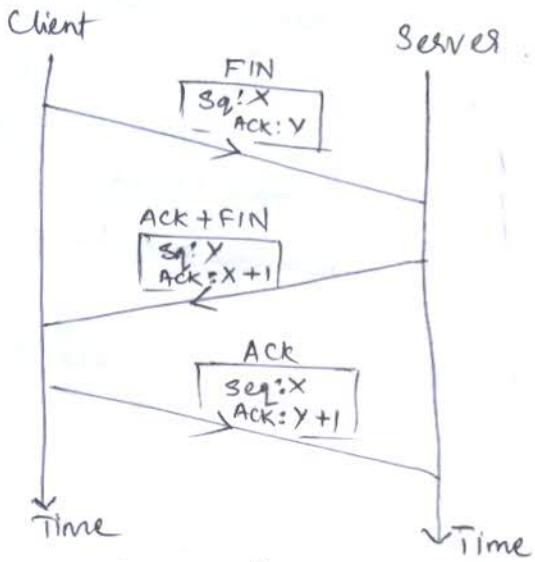
DOWNLOADED FROM KTUNOTES.IN

Connection Termination

Any of the two parties involved in exchanging data can close the connection. (usually initiated by the client)

* Two options for connection termination.
  1) Three-way Handshaking
  2) Four-way Handshaking with a half-close option.

Three-way Handshaking



Step ① : The client TCP, after receiving a close command from the client process, send FIN segment in which the FIN flag set

- FIN segment consumes one sequence number if it does not carry data.

Step ② The server TCP, after receiving the FIN segment, inform the process and sends the second segment FIN + ACK segment to confirm the receipt of FIN segment and at the same time to announce the closing of the connection in other direction.

- The FIN + ACK segment consumes one sequence number if it does not carry data.

Step ③ The client TCP sends the last segment, an Ack segment to confirm the receipt of FIN segment from the TCP server. This segment contains the acknowledgement number, which is 1 plus the sequence number received in the FIN segment from the server.

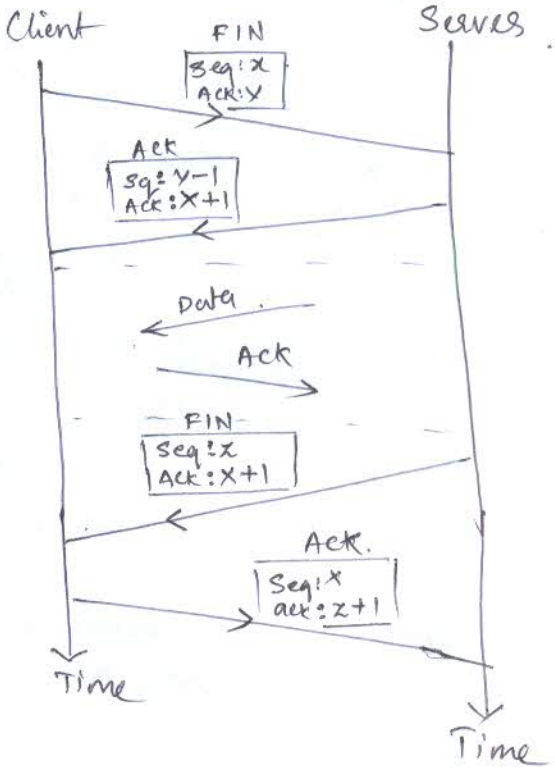
* Half close

- In TCP, one end can stop sending data while still receiving data.
- when a client sends data to the server to be ~~stored~~ sorted, the server to receive all the data before sorting can start. Client, after sending all data, can close the connection in the outbound direction. However, the inbound ~~data still needs time for sorting~~ direction must remain open to receive the sorted data.
- The client half-closes the connection by sending FIN segment. The server accepts the half close by sending ACK segment. The data transfer from the client to server stops. The server can still send data. when the server sent all the processed data. It send a FIN segment and acknowledged by client.

ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

(Half Close)



Flow control

A sliding window is used to make transmission more efficient as well as to control the flow of data, so that the destination does not become overwhelmed with data.
- TCP sliding window are byte-oriented.

* The size of the window is the lesser of receiver window (rwnd) and congestion window (cwnd)

window size = rwnd or cwnd (small value)

* Error detection and correction in TCP is achieved through the use of three simple tools
  1) checksum
  2) Acknowledgment
  3) Time-out

* Each segment includes a checksum field which is used to check for a corrupted segment. If the segment is corrupted, it is discarded by the destination TCP and considered as lost.
- TCP use a 16-bit checksum that is mandatory to every segment

* Acknowledgment: TCP use acknowledgement to confirm the receipt of the data segment
Ack segment do not consume sequence number and are not acknowledged

* Retransmission: a retransmission occurs if the retransmission timer expires or three duplicate Ack segments have arrived.
- No retransmission timer is set for an Ack segment.

* Data may arrive out of order and be temporarily stored by the receiving TCP, but TCP guarantees that no out-of-order segment is delivered to the process.

The state used in TCP connection

1) CLOSED
2) LISTEN
3) SYN RCVD
4) SYN SENT
5) ESTABLISHED
6) FIN WAIT 1
7) FIN WAIT 2
8) TIMED WAIT
10) CLOSE WAIT
11) LAST ACK

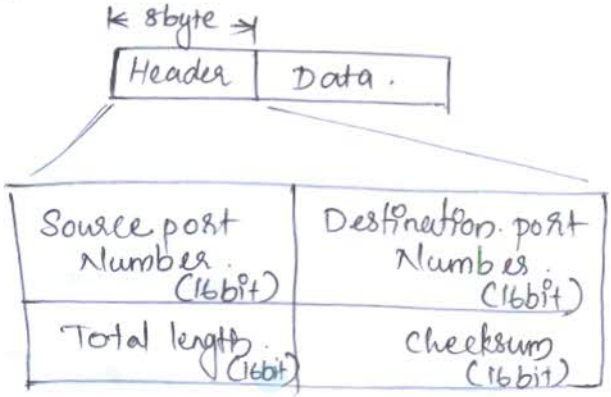
DOWNLOADED FROM KTUNOTES.IN

USER DATAGRAM PROTOCOL (UDP)

* The user datagram protocol is called a connectionless, unreliable transport protocol. It does not add anything to the service of IP except to provide process-to-process communication instead of host-to host communication.
* It performs very limited error checking.
* UDP is very simple protocol using minimum of overhead.
* does not care much about reliability.

User Datagram.

* UDP packets, called user datagrams.
* have fined-size header of 8 bytes.



Source port number (16 bit)
- Indicate the port of sending process.

Destination port (16 bit)
the port number used by the process running on the destination host

Total length (16 bit)
total length of the user datagram (data + Header)

UDP length = IP length − IP header's length

Checksum (16 bit)
used to detect errors over the entire user datagram. (header + data)

UDP operation.

* **Connectionless Services.**

UDP provides connectionless services, This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagram even if they are coming from the same source process and going to same process.

* user datagrams are not numbered.
* there is no connection establishment and no connection termination.
* each user datagram [illegible]th.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

Flow control and Error control

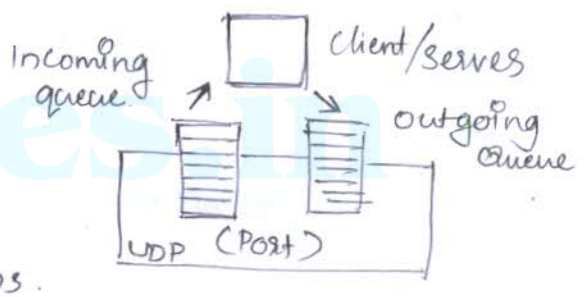
* UDP is a very simple, unreliable transport protocol. There is no flow control and hence no window mechanism.
* The receiver may overflow with incoming messages.
* There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a messages has been lost or duplicated.
* When the receiver detect an error through checksum the user datagram is silently discarded.

The lack of flow control and error control means that the process using ~~UDP~~ UDP should provide.

1) Encapsulation and Decapsulation.
2) Queuing.

Encapsulation and Decapsulation :- To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

Queuing :- Queues are associated with ports.



At the client site, when a process starts, it request a port number from the operating system. Some implementations create both an incoming and outgoing queue associated with each process.

The client process can send messages to outgoing queue by using the source port number specified in the request. UDP removes the message one by one and, after adding the UDP header, delivers them to IP

When a message arrives for client, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram. If there is such a queue. UDP sends the received user datagram to the end of the queue. If there is no such queue UDP discard the user datagram and ask ICMP protocol to send a port unreachable message to server.

Ktunotes.in

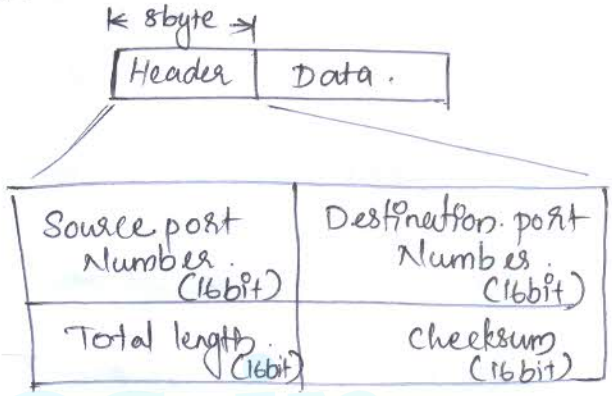
DOWNLOADED FROM KTUNOTES.IN

USER DATAGRAM PROTOCOL (UDP)

* The user datagram protocol is called a connectionless, unreliable transport protocol. It does not add anything to the service of IP except to provide process-to-process communication instead of host-to host communication.
* It performs very limited error checking.
* UDP is very simple protocol using minimum of overhead.
* does not care much about reliability.

User Datagram.

* UDP packets, called user datagrams.
* have fixed-size header of 8 bytes.



Source port number (16 bit)
- Indicate the port of sending process.

Destination port (16 bit)
the port number used by the process running on the destination host

Total length (16 bit)
total length of the user datagram (data + Header)

UDP length = IP length − IP header's length

Checksum (16bit)
used to detect errors over the entire user datagram. (header + data)

UDP operation.

* Connectionless services.

UDP provides connectionless services, This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagram even if they are coming from the same source process and going to same process.

* user datagrams are not numbered.
* there is no connection establishment and no connection termination.
* each user de[illegible]ath.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

Use of UDP

* UDP is suitable for a process that requires simple request-response communication with little concern for flow control and error control.
  - It is not usually used for a process such as FTP that need to send bulk data.
* UDP is suitable for a process with internal flow and error control Mechanisms.
  Eg:- Trivial file Transfer protocol (TFTP)
* UDP is suitable transport protocol for multicasting, Multicasting capability is embedded in the UDP software but not in the Tcp software.
* UDP is used for ~~Management~~ management processes such as SNMP
* UDP is used for some route updating protocols such as Routing Information protocol (RIP)

* Application layer.

The application layer enables the user, whether human or software, to access the network.

* The application layer is responsible for providing service to the user.
* The application layer receives services from transport layer.
* The application layer programs are based upon the concept of client and server
* For communication between client & server, addressing is needed when a client request a service from the server, it has to include the server address as destination address and its own address as source address. when a server responds, it reverses the address.
* Important application.
  1) Electronic mail
  2) World wide web.
  3) Multimedia
  4) Remote file transfer and access.

The most common service provided is SMTP or electronic mail. It allows the user to send a message to another user in Internet

MOUNT ZION COLLEGE OF ENGINEERING
Department of Computer Science & Information Technology
KADAMMANITTA

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

file transfer :- user can transfer a file from its compter to the server or transfer a file from a server to its computer.

—This application is called FTP.

* The client/server programs can be divided ~~into two~~ into two categories.

1) those that can be directly used by the user
eg: email.

2) those that support other application programs.

- DNS (Domain name system) is a supporting program that is used by other program such as email.

File Transfer protocol (FTP)

Transfering file from one computer to another is one of the most common task expected from a networking or internetworking

* Popular protocol involved in transferring file is, File transfer protocol (FTP)

* FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another.

- Some of the problems in transferring files from one system to the other are,

1) Two systems may use diffrent file name conventions
2) Two system may represent text and data in diffrent type
3) directory structures of the two systems may be different

FTP provides a simple solutions to all problems.

* FTP differs from other client/server application in that it establishes two connections between the host (make more efficient)

1) one connection is used for data transfer.
2) next is for control informations (Commands & Responses)

—The control connection use very simple rule of communication.

- transfer only one line of command or response at a time.

- Data connection uses more complex rules due to the variety of data types being transferred, complexity is at the FTP level. not TCP, For TCP both connections are treated the same.

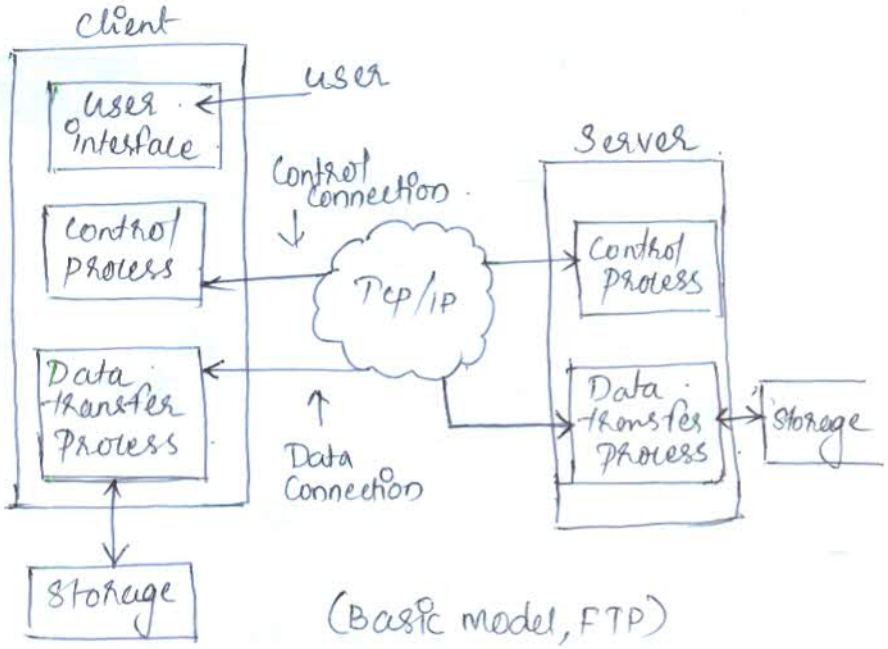
Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

* FTP uses the service of TCP. It need two Tcp connections. The well-known port 21 is used for the control connection and the well-known port 20 for the data connection.

* Client has three components.
  1) User Interface
  2) Control process
  3) Data transfer process.

* Server has two components.
  1) Server control process
  2) Server Data transfer process.



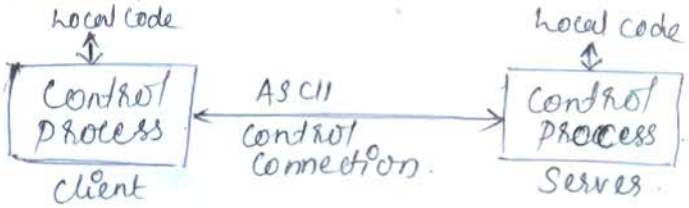
(Basic model, FTP)

- The control connection is made between the control processes. The data connection is made between the data transfer processes.
- The control connection remain connected during the entire interactive FTP session. The data connection is opened and the closed for each file transferred.

Note: when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times. If several files are transferred.

Communication over control connection

FTP uses a set of ASCII character to communicate across the control connection. Communication is achieved through comands and response.



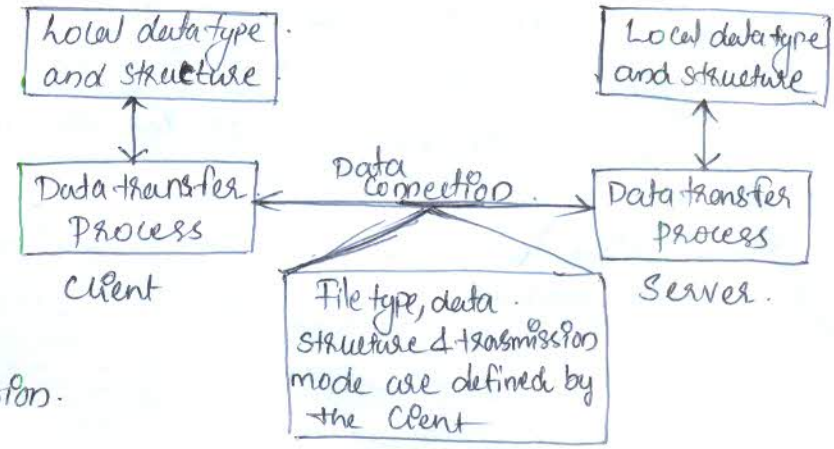
- One command is sent at a time. Each command or response is only of one short line. Therefore, it is not necessary to think about file structure.
- Each line is terminated with two characters end of line tokens.

Communication over Data Connection.

The purpose of implementing a data connection is to transfer file, For this client has to define the following
1) Type of file being transferred.
2) Structure of data.
3) Transmission mode

DOWNLOADED FROM KTUNOTES.IN

* File transfer occurs over the data connection under the control of the commands sent over the control connection.



* File transfer in FTP means.

1) A file is to copied from the server to the client. This is called retrieving a file. It is done under the supervision of the RETR command

2) A file is to be copied from the client to the server. This is called storing file, it is done under the supervision of the STOR command

3) A list of directory or file name is to be sent from the server to client. This is done under the supervision of the LIST command (FTP treats a list of directory or file name as a file)

* The client must define the type of file to be transferred, the structure of the data, and the transmission mode. Before sending the file through the data connection, Prepare a transmission through the control connection (RETR, STOR, LIST etc.)

* File types
  1) ASCII file
  2) EBCDIC file
  3) Image file.

ASCII file is the default format for transferring text file, EBCDIC file can be transferred if both end use EBCDIC encoding. Image file is the default format for transferring binary files. The file is sent as continuous stream of bits without any interpretation or encoding.

Note:- In ASCII file, Each character is encoded using 7-bit ASCII. The sender transforms the file into ASCII character and the receiver transform the ASCII characters to its own representation.

* Data Structure
  1) File structure (default)
  2) Record structure.
  3) Page structure.

File structure has no structure. It is simply a continuous stream of bytes. In the record structure, the file is divided into records. This can be used only with text files. In the page structure, the file divided into pages, which can be stored randomly or sequentially.

ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

* Transmission mode
  1) Stream mode
  2) Block mode
  3) Compressed mode

Stream mode :- The data is delivered from FTP to TCP in the form of continuous stream of bytes. TCP chops this data into segments of appropriate size.

Block mode :- data can be delivered from FTP to TCP in blocks. Each block is preceded by a 3 byte header

Compressed mode :- the data can be compressed, Generally, a run length encoding is used for compression.

* File Transfer
  1) Retreving a file. (RETR command)
  2) Storing of a file (STOR command)
  3) Retreving a List (LIST command)

* FTP Commands

	Commands	Meaning
FTP Commands to transfer files	Get	– copy a file from remote host to local host
	M. Get	– copy multiple file from remote host to local host
	put	– copy a file from local host to remote host
	M put	– copy multiple file from local host to remote host
FTP Commands to connect to a remote host	open	– Select the remote host and initiate high session.
	user	– Identify the remote user ID
	pass	– Authenticate the user.
	site	– Send the information to the remote host
FTP Commands to terminate session.	Quit	– Disconnect from the remote host & terminate FTP
	close	– Disconnect from the remote host but leave FTP client running.

Note :- Anonymous FTP

To use FTP, a users need an account and a password on the remote server. Some sites have a set of files available for public access, to enable anonymous FTP. To access this files, a user does not need to have an account or password.

user can use Anonymous as username and guest as password.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

Domain Name System (DNS)

IP addresses are convenient and compact way for identifying machines and are fundamental in TC/IP. It is unsuitable for human user. Meaningful hig-level symbolic names are more convenient for humans. Application software permit users to use symbolic names, but the underlaying network protocol require IP addresses.

ie, application layer need a address, which is high-level symbolic names (Each program will have its own address format)
(alias name)

* Application layer use names with proper syntax with efficient translation mechanism.
  - Domain name system (DNS) was invented for this purpose.

DNS – address mapped, alias name to IP address.

DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

DNS working

To map a name onto a IP address, an application program calls a library procedure called the resolver. The name is passed on to the resolver as a parameter, the resolver sends a UDP packet to local DNS server which look up the name and returns the corresponding IP address to the resolver. The resolver then sends this address to the caller, Then the program can establish a TCP connection with the destination or sends in the UDP packets.

Name space
- Flat Name space.
- Hierarchical Name space.

A name space that maps each address to unique name.

* Flat name space :- A name in this space is a sequence of characters without structure. The name may or may not have a common section; if they do, it has no meaning.
  - the main disadvantage of a flat name space is that it cannot be used in a large system such as Internet because it must be centrally controlled to avoid ambiguity and duplicate.

Hierarchical Name space :- name is made of several parts. the fist part can define the nature of the organization,

DOWNLOADED FROM KTUNOTES.IN

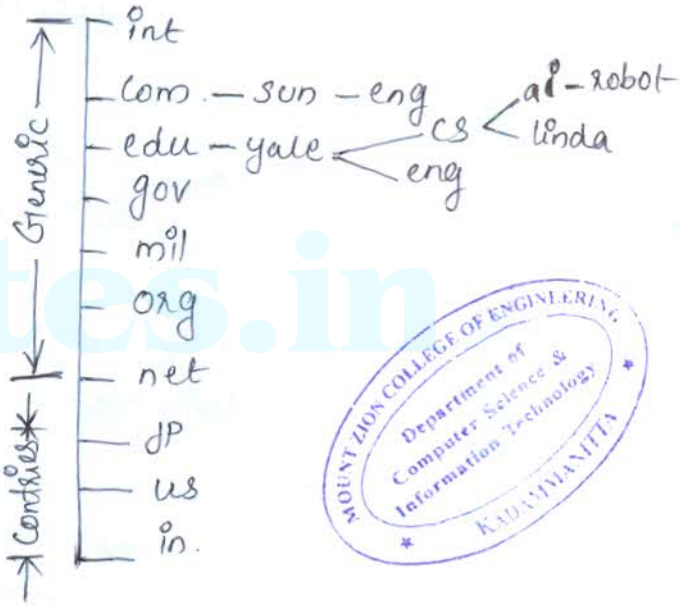
The second part can define the name of organization. the third part can define departments in the organization. and so on.
- the authority to assign and control the name spaces can be decentralized. A central authority can assign the part of the name that define the nature of organization and the name of organization. The responsibility of rest of name can be given to the organization itself.

* DNS Name space

Domain name space was designed from hierarchial name space.

Conceptually, the Internet has been divided into hundreds of top-level domains. Each domain covers many hosts. Each domain is divided into several subdomain and they are further divided and so on.

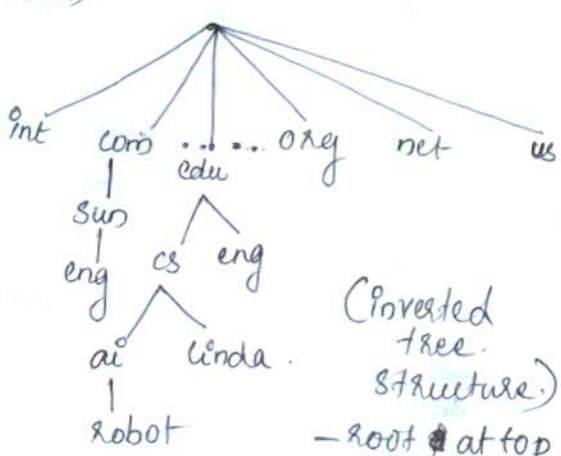
top-level domain < Generic, Countries



The Generic domain are com (commercial), edu (education), gov (government), int (International) mil (military), net (network provider) and org (non-profit organization).
The ~~Cont~~ country domain include for every ~~Cont~~ country.

MOUNT ZION COLLEGE OF ENGINEERING
Department of Computer Science & Information Technology
KADAMANITTA

* The components are separated by dots Eg:- eng.sun.com. this called hierarchical naming.
* Domain can be represented as tree (inverted) the tree can have only 128 levels, level 0 (root) to level (127)



(Inverted tree structure)
- root at top

Label

Each node in the tree has a label, which is a string with a maximum of 63 characters
The root label is null label (zero string)
DNS requires that branches from the same node have different labels, which guarantees the uniqueness of domain name.

DOWNLOADED FROM KTUNOTES.IN

Domain Name : Each node in the tree has a domain name. a full Domain Name is a sequence of labels separated by dots. the domain always read from the node up to the root. the last label is the labe of the root (null).

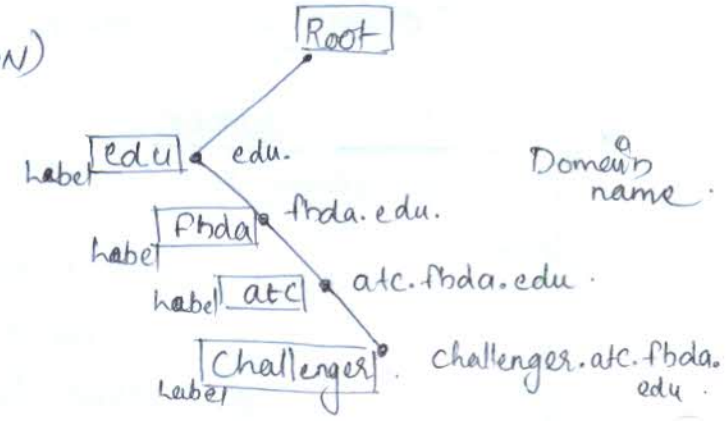
ie, last character is a dot. because the null string is nothing.

Fully Qualified Domain Name (FQDN)

If a label is terminated by a null string, it is called a fully Qualified domain name.

* FQDN is domain name that contains the full name of host. (It contain all labels)

Eg:- Challenger.atc.fbda.edu.



Partially Qualified Domain Name

If a label is not terminated by a null string, it is called a partially Qualified domain name (PQDN). A PQDN start from a node, but does not reach the root.

— Resolver can supply the missing part, called the Suffix to create FQDN

Eg:- user define pustial name., challenger.

the DNS client adds the suffix atc.fbda.edu before passing the address to DNS Server.

* The DNS client normally holds list of Suffixes.

Name Servers (Hierarchy of Name Servers)

* Name Server consist of DNS database, ie, the various name and their corresponding IP addresses. Theoretically, a single name Server could contain the entire DNS database. But practically to Store such a huge information at one place is inefficient and unreliable

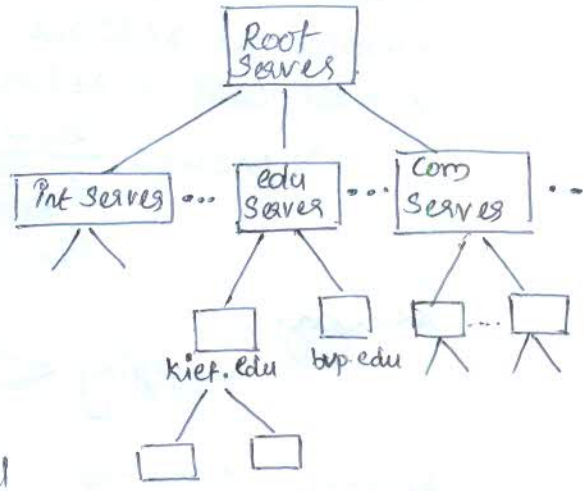
— ∴ distribute the information among many computers called DNS servers

In DNS server Hierarchy the whole Name space is divided into may first level domain, the first level domain are further divided into Smaller Subdomains. called Second level domain They can.

DOWNLOADED FROM KTUNOTES.IN

further divided and go on.

* The Root Server stand ~~along~~ alone.
* Each Server can be responsible to either large or small domain.
* The whole DNS Server / DNS name space is divided up into non-overlapping zones.
* A Server is responsible for or has authority over is called zone.



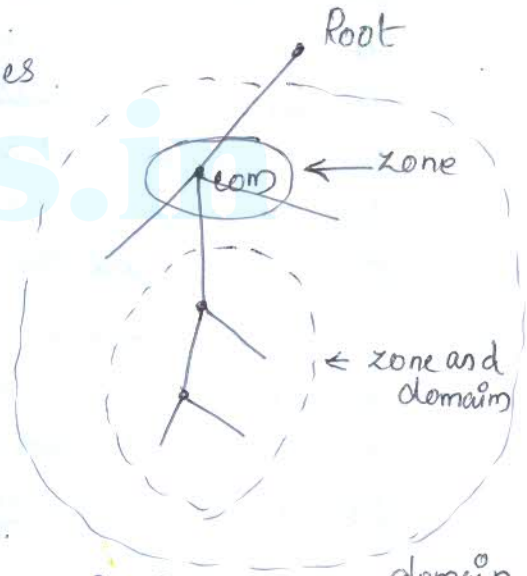
(Hierarchy of Name Server)

- If Server is appointed for a domain as zone and the domain is not further divided into subdomain then the domain and zone will be same.

* the Server make a data base ~~of~~ called a zone file

Root Server :- A root Server is a server whose zone consist of the whole DNS tree. It does not store any information about domains but delegates the authority to other servers. It keep the reference of these servers.

* There are more than 13 root servers and they are distributed all around the world.



Primary Server
It is a server which store a file about its zone. It is authorized to create, maintain and update the zone file. It store the zone file into local disk

Secondary Server.
this server ~~transform~~ transfers complete information about a zone from another server which may be primary or secondary.. the secondary server not authorized to create or update zone file.

* Secondary server load information from the primary servers.

Resolution
The process of mapping a name to an address or an address to a name is called as name address resolution.

DOWNLOADED FROM KTUNOTES.IN

Resolver :- DNS is the client server application. A host which wants to map a name to address or vise versa calls a DNS client named as resolver. When the name address mapping is necessary a host calls a resolver.

process → Request → Resolver → Request → Server
process ← Reply (Error-free) ← Resolver ← Reply ← Server

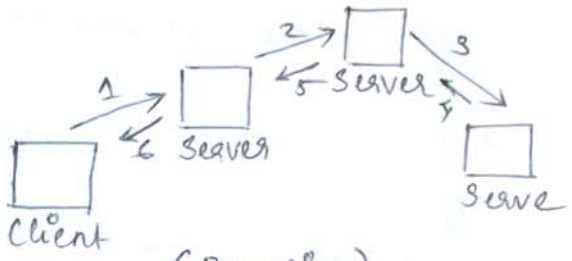
Mapping
- Name to address
- Address to Name

Recursive Resolution

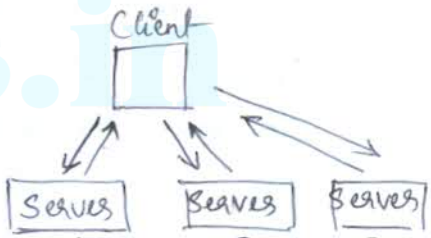
Sometimes, a client (resolver) request is recursive for a final resolution.

- If a server is authorised for a domain name, it checks it database and send reply. But if this server has not authorized. it divert the request to another server at wait for response. If the parent is an authority, it respond, other wise. Send the query to another server.
- When the query is solved, the response is return back to requesting client this query is called recursive query and process is called recursive resolution

Resolution
- Recursive Resolution
- Iterative Resolution.



(Recursive)



(Iterative)

Iterative Resolution

In Iterative resolution, if the server has authority for the name it will send the answer. But if it does not have the authority then it returns to the client, IP address of the server that it thinks has the answer for the query. The client has to repeat the query to this server. If server has also cannot answer it return the IP address of New server to client.

- this process is called Iterative Resolution.

Client sends the same query to different servers.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

ELECTRONIC MAIL

One of the most popular network service is electronic mail (e-mail). Simple Mail protocol (SMTP) is the standard mechanism for electronic mail in the internet.

* The first email system simply consisted by file transfer protocols. But some of the limitations of this system are.

1) Sending a message to a group of people was inconvenient
2) Message did not have any internal structure (Therefore, its computer processing was difficult).
3) The sender never used to know if a message arrived or not.
4) It was not easy to handover one's email to someone else.
5) It was not possible to create and send messages containing a text, drawing, fasmile and voice together.

Therefore, more elaborate e-mail system were proposed, ARPANET e-mail were published as RFC 821 (transmission protocol) and RFC822 (message format). These are used in Internet.

E-mail Architecture and services.

An e-mail system consists of two sub systems.

1) User agents. 2) Message transfer agents.

Ktunotes.in

User agents :- They allow the people to read and send e-mail

Message transfer agents :- They move the message from the source to the destination.

Basic functions :- E-mail systems support five basic systems ~~others~~.

1) composition. 2) Transfer. 3) Reporting
4) Displaying 5) Disposition.

Composition :- The process of creating messages and to answer them is known as composition. The system can also provide assistance with addressing and a number of header field attached to each message.

Transfer :- It is the process of moving messages from the sender to the recipient. This includes establishment of a connection from sender to destination or some intermediate machine outputting the message, and releasing the connection.

Reporting :- This is to tell the sender about whether the message was delivered or rejected or lost

DOWNLOADED FROM KTUNOTES.IN

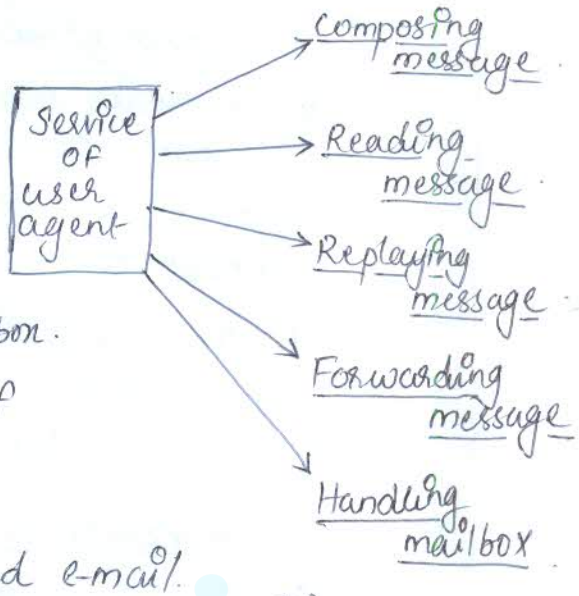
Displaying :- It is the process of displaying the incomming messages. For this purpose, simple conversion and formating are required to be done.

Disposition :- This is concerned with what recipient does with the message after receiving it. Some of the possibilities are.

1) Throw after reading. 2) Throw before reading.
3) Save message 4) Forward message 5) Process message in some other way.

Advanced Features of E-mail System.

1) Forwarding an e-mail to a person away from his computer.
2) Creating and destroying mailbones to store incoming e-mail.
3) Inspecting contents of mailbox, insert and delete message from the mailbox.
4) Sending a message to a large group of people using the idea of mail list
5) To provide registered e-mail.
6) Automatic notification of undelivered e-mail.
7) Carbon copies.
8) High priority e-mail
9) Secret (encrypted e-mail)
10) Alternative recipient.



E-mail Envelope.

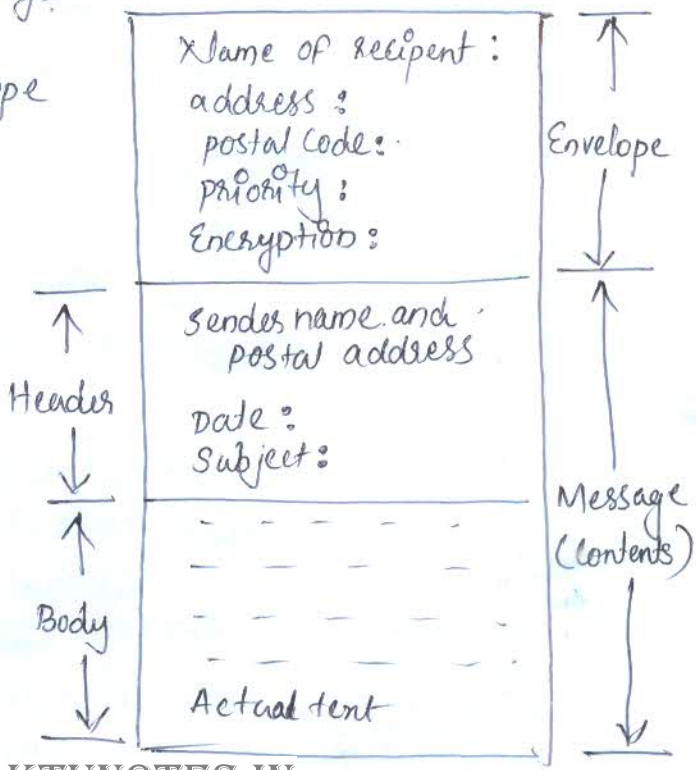
In modern e-mail system, there is distinction made between the e-mail envelope and contents. An e-mail envelope contains the message, destination address, priority, security level etc. The message transport agents use this envelope for routing.

Message.

The actual message inside the envelope is made of two parts.

1) Header 2) Body

Header carries the control information while body contains the message contents.



DOWNLOADED FROM KTUNOTES.IN

Message format – RFC 822.

Messages consist of a primitive envelope, some number of header field, a blank line and then the message body.

Header field logically consists of a single line of ASCII text which contains the field name, a colon and a field.

(RFC 822)

Header Name	Meaning
TO:	– E-mail address of primary recipients.
CC:	– E-mail address of secondary recipients.
BCC:	– E-mail address for blind carbon copies.
From:	– Person who create the message.
Sender:	– E-mail address of the actual sender.
Received:	– Line address by each transfer agent along the route.
Return-path:	– Can be used to identify the path back to the sender.
Date:	– The date and time of the message.
Reply to:	– E-mail address to which the reply is to be sent
Message-ID:	– Message identifying number.
In-Reply-TO:	– Message-Id of the message to which this is a reply
Reference:	– Other relevant message identification numbers.
Keywords:	– Keywords chosen by user.
Subject:	– Summary of the message for the one line display.

* Normally, the user agent builds a message and passes it to the message transfer agent which uses some header field for construct of envelope.

Message body

The message body comes after the header. The user can put whatever they want to send, in the message body. It is possible to terminate the message with ASCII cartoons, quotations etc.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME)

RS822 email used to consist of only the text messages in English and expressed in ASCII. But in the world wide Internet ~~envior~~ environment, this approach is not adequate.

* Some problems are encountered in sending and receiving the following types of messages.
  1) Messages in the languages having accents such as French or Germans.
  2) Messages which do not contain eg: audio and ~~video~~ video.
  3) Message in the languages which do not have alphabets. (eg: Chinese and japanese)
  4) Message is non latin alphabets such as Russian or Hebrew

The solution to these problem was MIME, (Multipurpose Internet Mail Extension) It was proposed in RFC 1341 and then updated in RFC 1521

Principle of MIME

MIME uses the same RFC 822 format but it adds structure to the message body (In RFC 822 there is no structure to the message body). In addition to this, MIME defines encoding rules for non ASCII message.

* MIME messages can be sent using the existing mail programs and protocols. The user can change sending and receiving programs themselves.

New-Message Headers.

Five new message Headers are defined for MIME.

1) MIME-version 2) Content-Type 3) Content-Transfer-Encoding
4) Content-Id 5) Content-Description

MIME-version :- It tell the user agent that the message is a MIME message and it also specifies the version of MIME being used.

Content-Type :- It is used to specify the type of message body. RFC1521 defines seven types with each one having one or more subtypes are separated by a slash.

Eg:- Video/mpeg

* The subtype must be given in the header.

DOWNLOADED FROM KTUNOTES.IN

Type	subtype	Description
Text	Plain	Text with unformatted Text
	Enriched	Text including simple formating Commands.
Image	Gif	Still pictures in GIF format
	Jpeg	Still picture in Jpeg format
Audio	Basic	Audible sound.
Video	MPeg	Movie in MPEG format
Application	Octet-stream	Byte sequence in unInterpreted form.
	post script	A printable document in post script.
Message	RFC822	A MIME RFC 822 message.
	partial	Split message for transmission.
	External body	Message itself should be fetched over the net.
Multipart	Mined	Independent part in specified Order.
	Alternative	Same message in different formats.
	Parallel	parts must be viewed simultaneously.
	Digist	Each part is complete RFC 822 message.

Content-Transfer-Encoding:- This header defines the method used to encode the messages into 0s and 1s. for transport.

	Type	Description
1)	7-bit	NVT ASCII character and short line.
2)	8-bit	non ASCII character and short line. Lines.
3)	Binary	non ASCII character with unlimited length.
4)	Base-64	6-bit blocks of data encoded into 8-bit ASCII character.
5)	Quoted-printable	non ASCII chereacters encoded as an equal sign followed by an ASCII code.

Content-ID :- This field identifies the contents. This header uniquely identifies the whole message in a multiple-message environment. Its format is same as the format of standard Message-ID header.

Content-Description :- This field tells the message is. It is in the form of ASCII string. This header is required because the recipient will know whether it is worth decoding and reading message.

(This header define whether the body is Image, audio or video also)

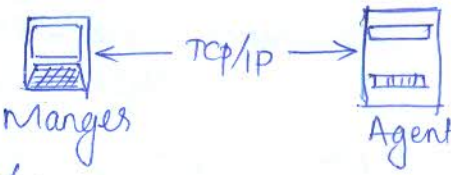
KTUNotes.in

DOWNLOADED FROM KTUNOTES.IN

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple network Management protocol (SNMP) may be defined as the framework for managing devices in Internet using the TCP/IP protocol suite.

* It provides a set of fundamental operations for monitoring and managing an Internet.
* SNMP uses the concept of manger and agent. a manager usually a host, control and monitors a set of agents, usually routers.
* SNMP is an application-level protocol in which a few manager stations control a set of agents.



* SNMP frees management task from both physical characteristics of the managed device and the underlying ~~ted~~ networking technology.

Concept of ~~Mang~~ Managers and Agents

A management station, called a manager, is a host that run the SNMP client program. A managed station, called Agent is a router (or a host) that run the SNMP server program Mangement is achieved through Simple interaction between manager and Agent.

* The agent keeps performance-information in a database. The manager has access to the values in the database.

Eg:- The ~~mang~~ manager can fetch and compare the numbes of packets received and forwarded to see if the router is congested or not.

* The server program running on the agent can check the environment and, if it notices something unusual, it can sent a warning message (called a trap) to manager.

- Management with SNMP is based on three basic ideas.

1) A manager checks an agent by requesting information that reflects the behavior of the agent

2) A manager forces an agent to perform a task by resetting values in the agent database.

3) An agent contributes to the management process by warning the manger of an unusual situation.

Ktunotes.in

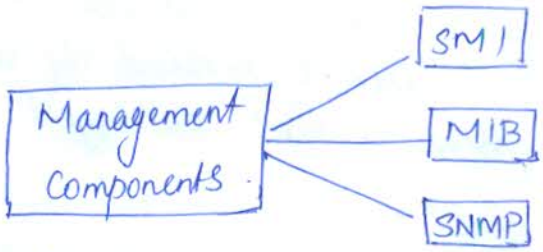
DOWNLOADED FROM KTUNOTES.IN

Internet Management Components.

Management in the internet is achieved not only through the SNMP Protocol but also by using other protocols that cooperate with SNMP.

* At top-level, management is accomplished with two other protocols.
  1) structure of Management information (SMI)
  2) Management information base (MIB)

* SNMP uses the services provided by the SMI & MIB protocols to do its job.
* SNMP, MIB & SMI use other protocols such as abstract syntax notation1 (ASN1) and basic encoding rules (BER)



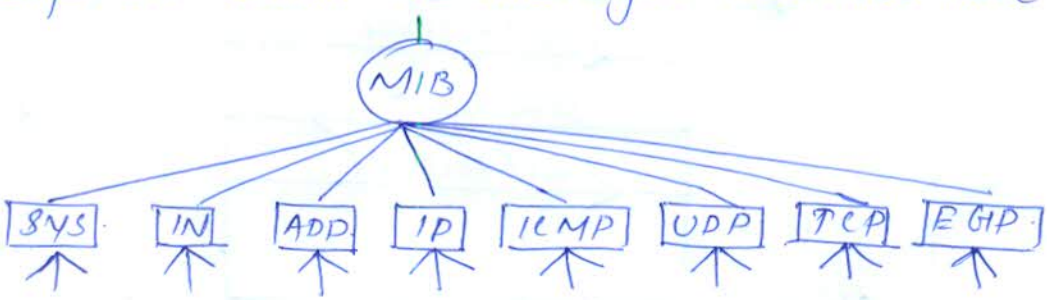
SMI :- The SMI is a component used in network management. Its functions are to name objects; to define the type of data that can be stored in an object, and to show how to encode data for transmission over the network.

MIB :- The management information base (MIB) is the second component used in network management. Each agent has its own MIB, which is a collection of all objects that the manager can manage

The objects in the MIB are categorized under eight different groups

1) System 2) interface 3) address translation 4) IP
5) ICMP 6) UDP 7) TCP 8) EGP

These groups are under the MIB object identifier tree.



SNMP : SNMP defines five messages.

1) Get Request 2) Get Next Request 3) Set Request
4) Get Response. 5) Trap.

DOWNLOADED FROM KTUNOTES.IN

Get Request :- The GetRequest message is sent from the manager (Client) to agent (server) to retrieve the value of a variable.

GetNext Request : The GetNext Request message is sent from the manager to agent to retrieve the value of varible. The retrieved value is the value of the object following the defined object in the message.

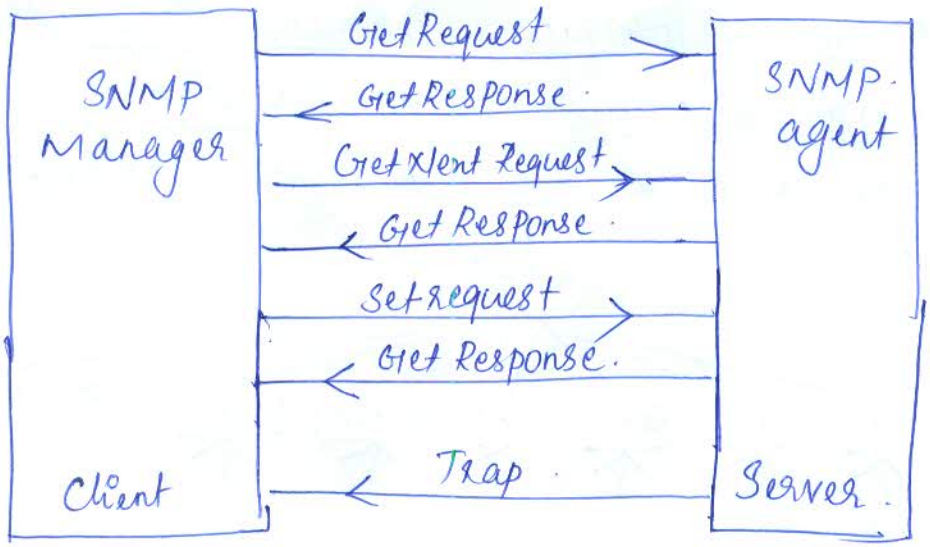
- It mostly used to retrieve the values of the entries in a table.
- If the manager does not know the indexes of entries, it cannot retrieve the values, However it can use GetNext Request and define the object.

Get Response :- The GetResponse message is sent from an agent to a manager in response to GetNext Request.
It contains the values of variables requested by the manager.

Set Request :- The Set Request message is sent from the manager to the agent to Set (store) a value in a variable.

Trap :- The trap message is sent from the agent to the manager to report an event.

Eg :- If the agent is rebooted, it informs the manager and reports the time of rebooting.



MOUNT ZION COLLEGE OF ENGINEERING
Department of Computer Science & Information Technology
KADAMMANITTA

DOWNLOADED FROM KTUNOTES.IN

CN

World Wide Web

- It is an architectural framework for accessing linked content spread out over millions of machines all over the internet.
- Easy for beginners to use & provide access with a rich graphical interface to an enormous wealth of information on almost every conceivable subject.
- Web began in 1989, first prototype operated ~~three~~ 18 months later. (Tim Berners Lee).
- First graphical browser called Mosaic was released in Feb 1993 by Marc ~~Ander~~ Andreessen.
- The period through 2000, when many web companies became worth hundreds of millions of dollars overnight only to go bust practically the next day when they turned out to be hype, even has a name, dot com era.

- W3C → World Wide Web Consortium.
  homepage → www.w3.org.

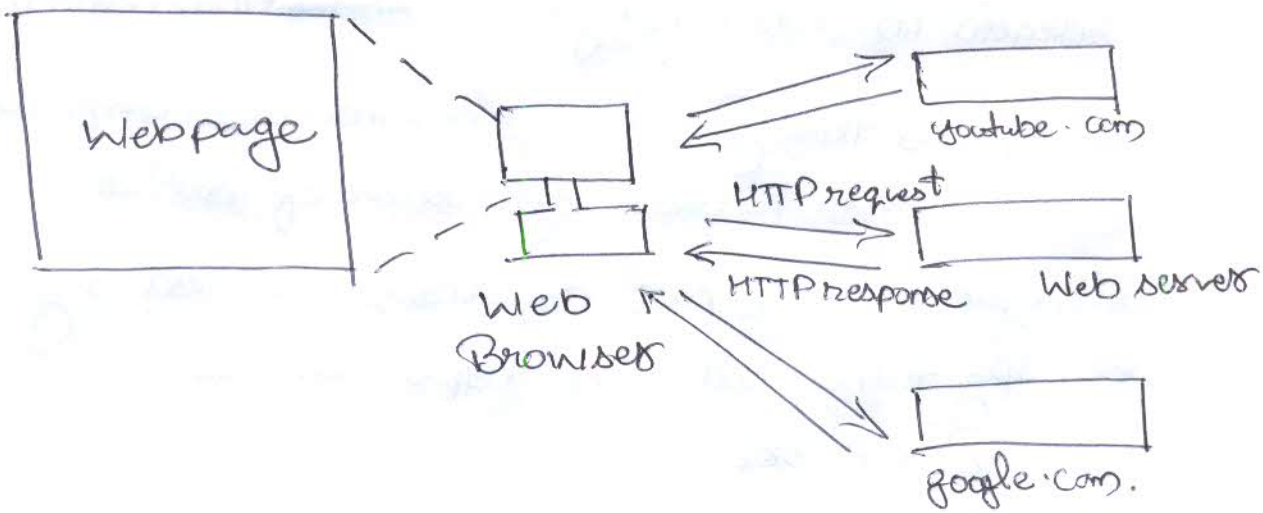
KTUNOTES.IN

DOWNLOADED FROM KTUNOTES.IN

Architectural Overview

- Web consists of vast worldwide collection of content in the form of webpages.
- The idea of having one page point to another, now called hypertext was invented by Vannevar Bush in 1945. (before internet was invented).
- Pages are viewed in a program called a browsers.
- Browsers fetches the page requested, interprets the content and displays the page properly formatted on the screen.
- A piece of text, icon, image and so on associated with links to other pages is called a hyperlink.

Ktunotes.in



- Page fetching is done by the browser without any help from the users.
- Each page is fetched by sending a request to one or more servers which respond with the contents of the page.

DOWNLOADED FROM KTUNOTES.IN

- The request-response protocol for fetching pages is a simple text based protocol that runs over TCP. It is called HTTP. (Hypertext Transfer Protocol).

- The content may simply be a document read off a disk, or result of database query & program execution.

- The page is a static page if it is a document that is the same everytime it is displayed.

- In contrast, if it was generated on demand by a program or set of programs it is a dynamic page.

- Dynamic page may present itself differently each time it is displayed. (eg: bookstore website).

- Cookie stores the information about which user likes what & prefers what to be bought or watched on web.

Client Side

- Each page on the web is assigned an URL (Uniform Resource Locator) that effectively serves as the page's worldwide name.

- URL has 3 parts:
  - → protocol ~~also~~ also known as schema
  - → DNS name of the machine on which the page is located.
  - → path uniquely indicating the specific page.

DOWNLOADED FROM KTUNOTES.IN

eg:

http://www.cs.washington.edu/index.html

protocol — DNS name of the host — path name

When an user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to.

Steps:

1. The browser determines the URL.
2. The browser asks DNS for the IP address of the server www.cs.washington.edu.
3. DNS replies with 128.208.3.88.
4. The browser makes a TCP connection to 128.208.3.88 on port 80 the well known port of the HTTP protocol.
5. It sends over an HTTP request asking for page /index.html
6. The www.cs.washington.edu server sends the page as an HTTP response, for example, by sending the file /index.html.
7. If the pages include URLs that are needed for display, the browser fetches the other URLs using the same process.
8. The browser displays the page.
9. The TCP connections are released if there are no other requests to the same servers for a short period.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

- The http protocol is the web's native language, the one spoken by web servers.
- FTP protocol is used to access files by FTP, file transfer protocol. Web makes it easy to obtain files placed on numerous FTP servers throughout the world by providing a simple, clickable interface instead of command line interface.
- The Mailto protocol does not fetch webpages but allows users to send email from a web browser.
- RTSP and SIP protocols are for establishing streaming media sessions & audio & video calls.
- URLs are generalized into URIs (Uniform Resource Identifiers). Some URIs tell how to identify or locate ~~es~~ a resource. while others tell the name of the resource but not where to find out. Such URIs are called URNs (Uniform Resource Names).

- To be able to display a webpage, the browser has to understand its format. Webpages are written in a standardized language called HTML.

- Browser consults the table of MIME types to recognize the type of files used in the webpage.

DOWNLOADED FROM KTUNOTES.IN

- A plug in or helper applications can be used for this purpose. A plugin is a third-party code module that is installed as an extension to the browsers. Common examples are PDF, Flash etc.

- Helper application is a complete program running as a separate process. It usually just accepts the name of a scratch file where the content file has been stored, opens the file & displays the content.

SERVER SIDE

The server is given the name of a file to lookup and return via the network. (In both cases) the steps that the server performs in its main loop are:

1. Accept a TCP connection from the client.
2. Get the path to the page which is the name of file requested.
3. Get the file.
4. Send the contents of the file to the client.
5. Release the TCP connection.

KTUnotes.in

DOWNLOADED FROM KTUNOTES.IN

- Web servers are implemented with a different design to serve many requests per second. One problem with the simple design is that accessing files is often the bottleneck.

Issues:

1. Disk reads are very slow compared to execution.
2. Same files may be read repeatedly using operating system calls.
3. Only one request is processed at a time.

- Make the server multithreaded to tackle the problem of serving a single request at a time.

> Steps that occur after the TCP connection / any secure transport mechanism have been established.

1. Resolve the name of the webpage requested.
2. Perform access control on the webpage.
3. Check the cache.
4. Fetch the requested page from disk or run a program to build it.
5. Determine the rest of the resource. ← (eg: MIME)
6. Return the ~~resp~~ response to the client.
7. Make an entry in the server log.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

STATIC WEBPAGE

The basis of the web transferring web pages from servers to client. Web pages are static. That is, they are just files sitting on some servers that present themselves in the same way each time they are fetched and viewed. A page containing a video can be static webpage.

HTML

- HTML was introduced with web. It allows users to produce webpages that include text, graphics, video, pointers to other webpages and more.
- HTML is a markup language or a language for describing how the documents are formatted.
- A webpage consists of head & body each enclosed by tags although most browsers do not complain if the tags are missing.

CSS

- Cascading Style sheets introduced style sheets to the web with HTML 4.0.
- CSS defines a language for describing rules that control the appearance of tagged content.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

Dynamic Webpages and Web Applications

- Web is being used for applications and services such as buying products on e commerce sites, exploring maps etc. The twist ~~in~~ is that these applications run inside the browsers with user data stored on servers in internet data centers.

  They use web protocols to access information via the internet and the browser to display a user interface.

- The advantage is that users do not need to install separate applications and user data can be ~~accessed~~ accessed from different computers and backed up by the service providers. This model is a prevalent form of cloud computing.

Ktunotes.in

Server Side.

Standard API's have been developed for webservers to invoke programs. The existence of these interfaces make it easier for developers to extend different ~~webpage~~ servers with web applications.

- First API method for handling dynamic page requests which was available since beginning is called CGI or Common Gateway Interface.

- CGI provides an interface to allow webservers to talk to back-end programs & scripts that can accept i/p & generate HTML pages in response.

DOWNLOADED FROM KTUNOTES.IN

- A popular language for writing these scripts is PHP (Hypertext preprocessor). To use it, the server has to understand PHP, just as a browser has to understand CSS to ~~inte~~ interpret webpages with style sheets.

- JSP (JavaServer Page) is similar to PHP except that the dynamic part is written in the java programming language instead of PHP.

- ASP.NET (Active Server Page.Net) is Microsoft's version of PHP & javaserver page. It uses programs written in Microsoft's proprietary .NET networked application framework for generating the dynamic content.

Client Side

- CGI & PHP scripts solve the problem of handling i/p & interactions with databases on the server. but none of them can interact with users directly. The technologies used to produce interactive webpages are broadly referred to as dynamic HTML.

- Most popular scripting language for the client side is JavaScript. It is a high level language.

- An alternative to javascript on windows is VBScript which is based on visual basic.

- Another popular method is use of applets for a virtual computer called JVM.

- ActiveX controls used by Microsoft instead of java applets.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN

MODULE V

Internet Control Protocols – ICMP, ARP, RARP, BOOTP. Internet Multicasting – IGMP, Exterior Routing Protocols – BGP. IPv6 – Addressing – Issues, ICMPv6.

The Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP, and DHCP.

ICMP - The Internet Control Message Protocol

The operation of the Internet is monitored closely by the routers. When something unexpected occurs, the event is reported by the ICMP (Internet Control Message Protocol), which is also used to test the Internet. Each ICMP message type is encapsulated in an IP packet.

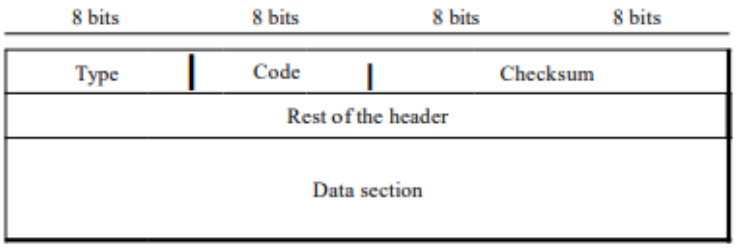
Types of messages:
ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages.**

- The **error-reporting messages** report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The **query messages**, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors

Message Format
An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all.

Ktunotes.in

Figure 21.8 *Generalformat of[CM? messages*

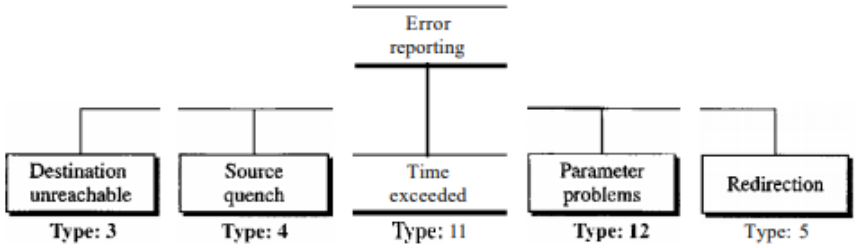


ICMP type, defines the type of the message.
The **code field** specifies the reason for the particular message type.
The last common field is the **checksum field** for error handling.
The **rest of the header** is specific for each message type.
The **data section** in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query.

One of the main responsibilities of ICMP is to report errors. ICMP always reports error messages to the original source. Five types of errors are handled: destination unreachable, source quench, time exceeded, parameter problems, and redirection

DOWNLOADED FROM KTUNOTES.IN

Figure 21.9 *Error-reporting messages*



The following are **important points about ICMP error messages:**

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source, which receives the error message, informa tion about the datagram itself. The 8 bytes of data are included because on UDP and TCP protocols, the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error.

The **DESTINATION UNREACHABLE** message is used

- when the subnet or a router cannot locate the destination or
- when a packet with the DF bit cannot be delivered because a "small-packet" network stands in the way.

The **TIME EXCEEDED** message is sent
The time-exceeded message is generated in two cases:

- routers use routing tables to find the next hop (next router) that must receive the packet. If there are errors in one or more routing tables, a packet can travel in a loop or a cycle, going from one router to the next or visiting a series of routers endlessly. Each datagram contains a field called time to live that controls this situation. When a datagram visits a router, the value of this field is decremented by 1. When the time-to-live value reaches 0, after decrementing, the router discards the datagram. How ever, when the datagram is discarded, a time-exceeded message must be sent by the router to the original source. Second, a time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit.
- when a packet is dropped because its counter has reached zero.
- This event is a symptom that packets are looping, that there is enormous congestion, or
- The timer values are being set too low.

DOWNLOADED FROM KTUNOTES.IN

- If there are errors in one or more routing tables, a packet can travel in a loop or a cycle, going from one router to the next or visiting a series of routers endlessly. each datagram contains a field called time to live that controls this situation. When a datagram visits a router, the value of this field is decremented by 1. When the time-to-live value reaches 0, after decrementing, the router discards the datagram. However, when the datagram is discarded, a time-exceeded message must be sent by the router to the original source. Second, a time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit.

The **PARAMETER PROBLEM** message indicates

- an illegal value has been detected in a header field.
- A bug in the sending host's IP software or possibly in the software of a router transited.
- If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.
- Any ambiguity in the header part of a datagram can Create serious problems as the data gram travels through the Internet. If a router or the destination host discovers an ambig uous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.

The **SOURCE QUENCH** message was used

- to throttle hosts that were sending too many packets. When a host received this message, it was expected to slow down. It is rarely used any more because when congestion occurs, these packets tend to worsen it.
- The source-quench message in ICMP was designed to add a kind of flow control to the IP. When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram. This message has two purposes. First, it informs the source that the datagram has been discarded. Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.
- The IP protocol is a connectionless protocol. There is no communication between the source host, which produces the datagram, the routers, which forward it, and the destination host, which processes it. One of the ramifications of this absence of communication is the lack of flow control. IP does not have a flow control mechanism embedded in the protocol. The lack of flow control can create a major problem in the operation of IP: congestion. The source host never knows if the routers or the destination host has been overwhelmed with datagrams. The source host never knows if it is producing datagrams faster than can be forwarded by routers or processed by the destination host. The lack of flow control can create congestion in routers or the destination host. A router or a host has a limited-size queue (buffer) for incoming datagrams waiting to be forwarded (in the case of a router) or to be processed (in the case of a host). If the datagrams are received much faster than they can be forwarded or processed, the queue may overflow. In this case, the router or the host has no choice but to discard some of the datagrams. The source-quench message in ICMP was designed to add a kind of flow control to the IP. When a router or host discards a datagram due to con gestion, it sends a source-quench message to the sender of the datagram. This

DOWNLOADED FROM KTUNOTES.IN

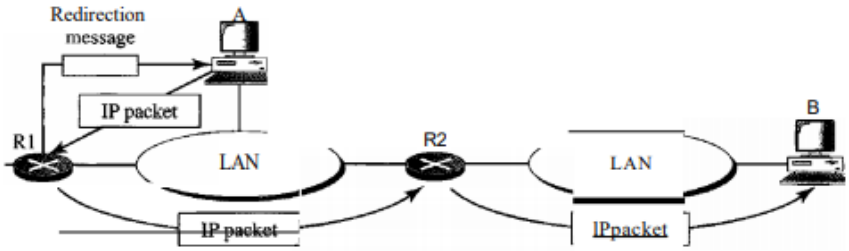
message has two purposes. First, it informs the source that the datagram has been discarded. Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.

The **REDIRECT** message is used

- when a router notices that a packet seems to be routed wrong. It is used by the router to tell the sending host about the probable error.
- When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router. The same is true if the sender is a host. Both routers and hosts, then, must have a routing table to find the address of the router or the next router. Routing is dynamic.
- However, for efficiency, hosts do not take part in the routing update process because there are many more hosts in an internet than routerS. Updating the routing tables of hosts dynamically produces unacceptable traffic. The hosts usually use static routing. When a host comes up, its routing table has a limited number of entries. It usually knows the IP address of only one router, the default router. For this reason, the host may send a data gram, which is destined for another network, to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router. However, to update the routing table of the host, it sends a redirection message to the host. This concept of redirection is shown in Figure 21.11. Host A wants to send a datagram to host B.

Ktunotes.in

Figure **21.11** *Redirection concept*



- Router R2 is obviously the most efficient routing choice, but host A did not choose router R2. The datagram goes to R1 instead. Router R1, after consulting its table, finds that the packet should have gone to R2. It sends the packet to R2 and, at the same time, sends a redirection message to host A. Host A's routing table can now be updated.

Query

ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages, as shown in Figure 21.12. In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet, which in tum is encapsulated in a data link layer frame.

DOWNLOADED FROM KTUNOTES.IN

Figure 21.12 *Query messages*

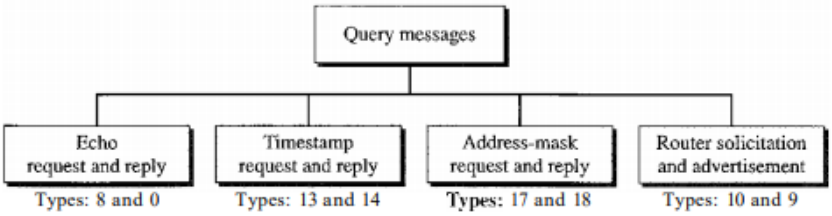
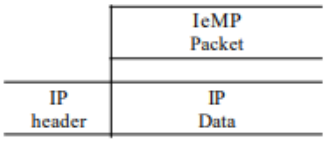


Figure 21.13 *Encapsulation ofICMP query messages*



The **ECHO and ECHO REPLY** messages are used to

- see if a given destination is reachable and alive.
- Upon receiving the ECHO message, the destination is expected to send an ECHO REPLY message back.
- The echo-request and echo-reply messages are designed for diagnostic purposes. Network managers and users utilize this pair of messages to identify network problems. The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other. The echo-request and echo-reply messages can be used to determine if there is communication at the IP level. Because ICMP messages are encapsulated in IP datagrams, the receipt of an echo-reply message by the machine that sent the echo request is proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram. Also, it is proof that the intermediate routers are receiving, processing, and forwarding IP datagrams

The **TIMESTAMP REQUEST and TIMESTAMP REPLY** messages are similar,

- except that the arrival time of the message and the departure time of the reply are recorded in the reply.
- This facility is used to measure network performance.
- Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.

ADDRESS-MASK REQUEST AND REPLY

A host may know its IP address, but it may not know the corresponding mask. For example, a host may know its IP address as 159.31.17.24, but it may not know that the corresponding mask is /24. To obtain its mask, a host sends an address-mask-request message to a router on the LAN.

DOWNLOADED FROM KTUNOTES.IN

If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message. The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary

ROUTER SOLICITATION AND ADVERTISEMENT

A host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation. A host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message. A router can also periodically send router-advertisement messages even if no host has solic ited. Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

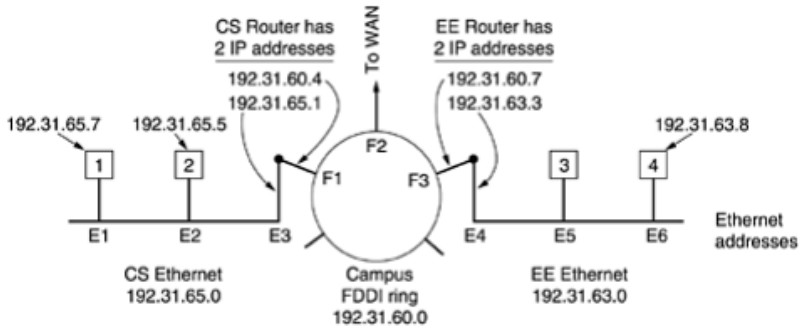
ARP—The Address Resolution Protocol - ARP solves the problem of finding out which Ethernet address corresponds to a given IP address.

Every machine on the Internet has one (or more) IP addresses, these cannot actually be used for sending packets because the data link layer hardware does not understand Internet addresses. Most hosts at organizations are attached to a LAN by an interface board that only understands LAN addresses. For example, every Ethernet board ever manufactured comes equipped with a unique 48-bit Ethernet address. The boards send and receive frames based on 48-bit Ethernet addresses.

Ktunotes.in

How do IP addresses get mapped onto data link layer addresses, such as Ethernet?

Figure 5-62. Three interconnected /24 networks: two Ethernets and an FDDI ring.



Small university with several class C (now called /24) networks is illustrated. We have two Ethernets, one in the Computer Science Dept., with IP address 192.31.65.0 and one in Electrical Engineering, with IP address 192.31.63.0. These are connected by a campus backbone ring (e.g., FDDI) with IP address 192.31.60.0. Each machine on an Ethernet has a unique Ethernet address, labeled E1 through E6, and each machine on the FDDI ring has an FDDI address, labeled F1 through F3.

- **a user on host 1 sends a packet to a user on host 2:**

1. assume the sender knows the name of the intended receiver, eg:mary@eagle.cs.uni.edu
2. find the IP address for host 2, known as eagle.cs.uni.edu.

DOWNLOADED FROM KTUNOTES.IN

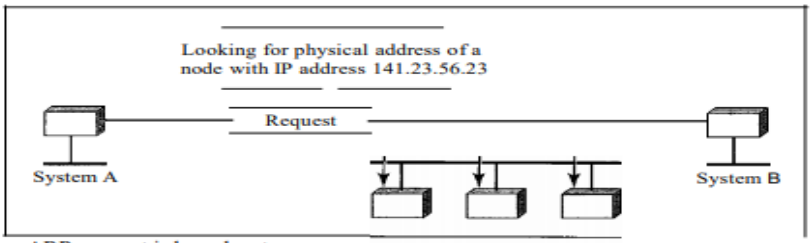
3. This lookup is performed by the Domain Name System, that DNS returns the IP address for host 2 (192.31.65.5).
4. The upper layer software on host 1 now builds a packet with 192.31.65.5 in the Destination address field and gives it to the IP software to transmit
5. The IP software can look at the address and see that the destination is on its own network, but it needs to find the destination's Ethernet address:

- One solution is to have a **configuration file/static mapping** somewhere in the system that maps IP addresses onto Ethernet addresses. While this solution is certainly possible, for organizations with thousands of machines, keeping all these files up to date is an error-prone, time-consuming job. Limitations of static mapping:
    - 1. A machine could change its NIC, resulting in a new physical address.
    - 2. In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.
    - 3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.
    - To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance
- Host 1 to output a broadcast packet onto the Ethernet asking: Who owns IP address 192.31.65.5? The broadcast will arrive at every machine on Ethernet 192.31.65.0, and each one will check its IP address. Host 2 alone will respond with its Ethernet address (E2). The protocol used for asking this question and getting the reply is called **ARP (Address Resolution Protocol).** Almost every machine on the Internet runs it. ARP is defined in RFC 826.
- The advantage of using ARP over configuration files is the simplicity. The system manager does not have to do much except assign each machine an IP address and decide about subnet masks. ARP does the rest.

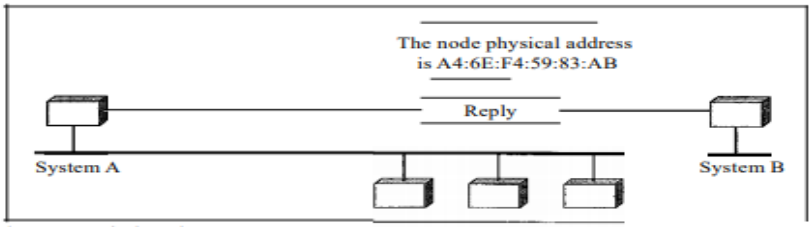
6. The IP software on host 1 builds an Ethernet frame addressed to E2, puts the IP packet (addressed to 192.31.65.5) in the payload field, and dumps it onto the Ethernet.
7. The Ethernet board of host 2 detects this frame, recognizes it as a frame for itself, scoops it up, and causes an interrupt.
8. The Ethernet driver extracts the IP packet from the payload and passes it to the IP software, which sees that it is correctly addressed and processes it.

DOWNLOADED FROM KTUNOTES.IN

Figure 21.1 *ARP operation*



a. ARP request is broadcast



b. ARP reply is unicast

Optimizations to make ARP work more efficiently:

- All machines on the Ethernet can enter this mapping into their ARP caches.

1. Once a machine has run ARP, it caches the result in case it needs to contact the same machine shortly. Next time it will find the mapping in its own cache, thus eliminating the need for a second broadcast.
2. Host 2 will need to send back a reply, forcing it, too, to run ARP to determine the sender's Ethernet address. This ARP broadcast can be avoided by having host 1 include its IP-to-Ethernet mapping in the ARP packet. When the ARP broadcast arrives at host 2, the pair (192.31.65.7, E1) is entered into host 2's ARP cache for future use.

- Every machine broadcast its mapping when it boots. This broadcast is generally done in the form of an ARP looking for its own IP address. There should not be a response, but a side effect of the broadcast is to make an entry in everyone's ARP cache. If a response does (unexpectedly) arrive, two machines have been assigned the same IP address. The new one should inform the system manager and not boot.
- every machine broadcast its mapping when it boots. This broadcast is generally done in the form of an ARP looking for its own IP address. There should not be a response, but a side effect of the broadcast is to make an entry in everyone's ARP cache. If a response does (unexpectedly) arrive, two machines have been assigned the same IP address. The new one should inform the system manager and not boot.

- **host 1 wants to send a packet to host 4 (192.31.63.8) / From host 1 to a distant network over a WAN :**

Using ARP will fail because host 4 will not see the broadcast (routers do not forward Ethernet-level broadcasts). There are two solutions:

1. First, the CS router could be configured to respond to ARP requests for network 192.31.63.0 (and possibly other local networks). In this case, host 1 will make an ARP cache entry of (192.31.63.8, E3) and send all traffic for host 4 to the local router. This solution is called **proxy ARP**.

DOWNLOADED FROM KTUNOTES.IN

2. The second solution is to have host 1 immediately see that the destination is on a remote network and just send all such traffic to a default Ethernet address that handles all remote traffic, in this case E3. This solution does not require having the CS router know which remote networks it is serving.

Either way, host 1 packs the IP packet into the payload field of an Ethernet frame addressed to E3. When the CS router gets the Ethernet frame, it removes the IP packet from the payload field and looks up the IP address in its routing tables. It discovers that packets for network 192.31.63.0 are supposed to go to router 192.31.60.7. If it does not already know the FDDI address of 192.31.60.7, it broadcasts an ARP packet onto the ring and learns that its ring address is F3. It then inserts the packet into the payload field of an FDDI frame addressed to F3 and puts it on the ring.

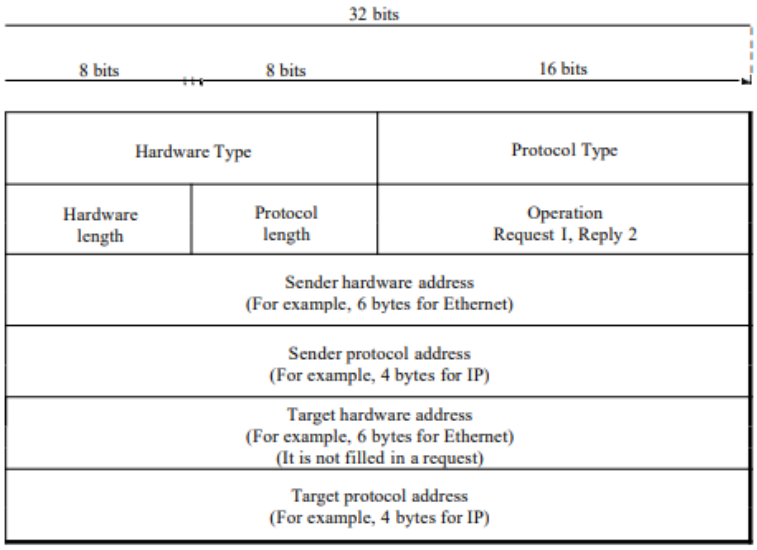
At the EE router, the FDDI driver removes the packet from the payload field and gives it to the IP software, which sees that it needs to send the packet to 192.31.63.8. If this IP address is not in its ARP cache, it broadcasts an ARP request on the EE Ethernet and learns that the destination address is E6,soit builds an Ethernet frame addressed to E6, puts the packet in the payload field, and sends it over the Ethernet. When the Ethernet frame arrives at host 4, the packet is extracted from the frame and passed to the IP software for processing.

From host 1 to a distant network over a WAN works essentially the same way, except that this time the CS router's tables tell it to use the WAN router whose FDDI address is F2.

Ktunotes.in

ARP PACKET

Figure 21.2 *ARP packet*



Hardware type. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1.
Protocol type. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 080016.

DOWNLOADED FROM KTUNOTES.IN

Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) and ARP reply (2).
Sender hardware address. This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
Target hardware address. This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is alI Os because the sender does not know the physical address of the target.
Target protocol address. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

Operation
These are the steps involved in an ARP process:
1. The sender knows the IP address of the target.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with Os.
3. The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as the source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes its IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine.
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

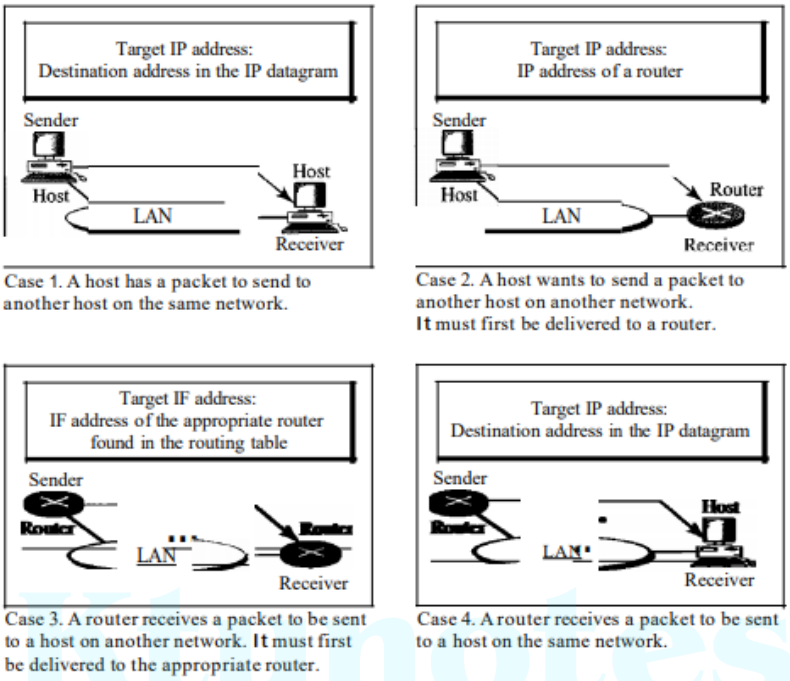
KTUNotes.in

DOWNLOADED FROM KTUNOTES.IN

Four Different Cases

The following are four different cases in which the services of ARP can be used (see Figure 21.4).

Figure 21.4 *Four cases using ARP*



Case 1. A host has a packet to send to another host on the same network.

Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.

Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

Case 4. A router receives a packet to be sent to a host on the same network.

1. The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header
2. The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. Ifit does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.
3. The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.
4. The sender is a router that has received a datagram destined for a host on the same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

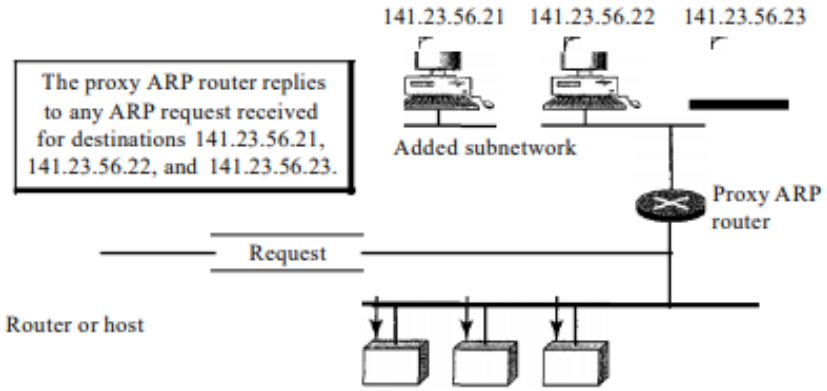
An ARP request is broadcast; an ARP reply is unicast.

ProxyARP

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router.

DOWNLOADED FROM KTUNOTES.IN

Figure 21.6 *Proxy ARP*



In Figure 21.6 the ARP installed on the right-hand host will answer only to anARP request with a target IP address of 141.23.56.23.

The administrator may need to create a subnet without changing the whole system to recognize subnetted addresses. One solution is to add a router running a proxy ARP. In this case, the router acts on behalf of all the hosts installed on the subnet. When it receives an ARP request with a target IP address that matches the address of one of its proteges (141.23.56.21, 141.23.56.22, or 141.23.56.23), it sends an ARP reply and announces its hardware address as the target hardware address. When the router receives the IP packet, it sends the packet to the appropriate host.

Mapping Physical to Logical Address:

RARP, BOOTP, and DHCP There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease

RARP - Reverse Address Resolution Protocol - (defined in RFC 903)

Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine.

To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file. However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator

DOWNLOADED FROM KTUNOTES.IN

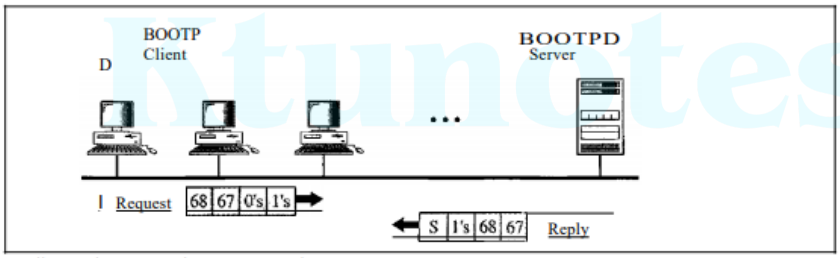
The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply. The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

There is a serious problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, allis in the case of Ethernet, does not pass the boundaries of a network. This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete. Two protocols, BOOTP and DHCp, are replacing RARP.

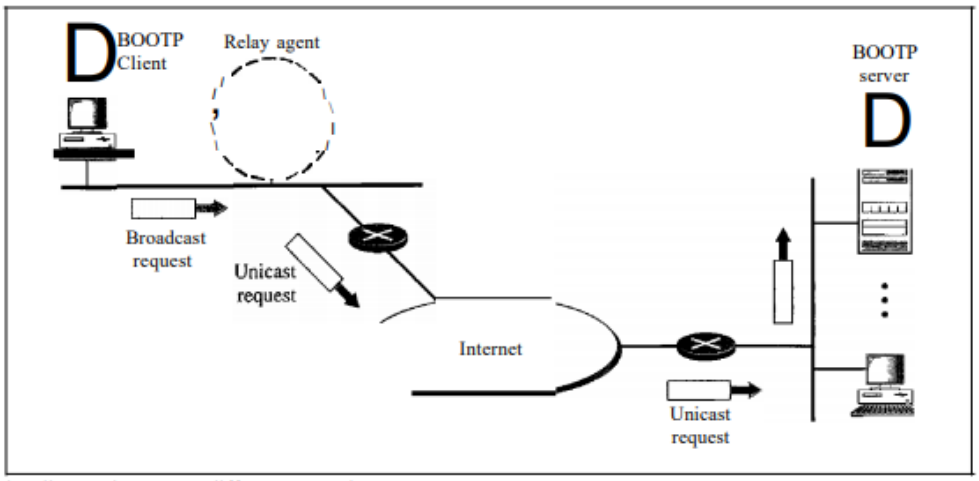
BOOTP

The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks, as shown in Figure 21.7. BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.

Figure 21.7 *BOOTP client and server on the same and different network*



a. Client and server on the same network



b. Client and server on different networks

A client can send an IP datagram when it knows neither its own IP address (the source address) nor the server's IP address (the destination address) by using all 1 as as the source address and all 1s as the destination address.

DOWNLOADED FROM KTUNOTES.IN

One of the advantages of BOOTP over RARP is that the client and server are application-layer processes.

One problem that must be solved. The BOOTP request is broadcast because the client does not know the IP address of the server. A broadcast IP datagram cannot pass through any router. To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay. The host in this case is called **a relay agent**. The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server. The packet, carrying a unicast destination address, is routed by any router and reaches the BOOTP server. The BOOTP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent. The relay agent, after receiving the reply, sends it to the BOOTP client.

BOOTP is not a dynamic configuration protocol. When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address. This implies that the binding between the physical address and the IP address of the client already exists. The binding is predetermined.

If a host moves from one physical network to another. If a host wants a temporary IP address. BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator. BOOTP is a static configuration protocol

Ktunotes.in

Internet Multicasting – IGMP:

The IP protocol can be involved in two types of communication**: unicasting** and **multicasting**. **Unicasting** is the communication between one sender and one receiver. It is a one-to-one communication. Processes which send the same message to a large number of receivers simultaneously is called **multicasting**, which is a one-to-many communication. Examples are updating replicated, distributed databases, transmitting stock quotes to multiple brokers, and handling digital conference (i.e., multiparty) telephone calls.

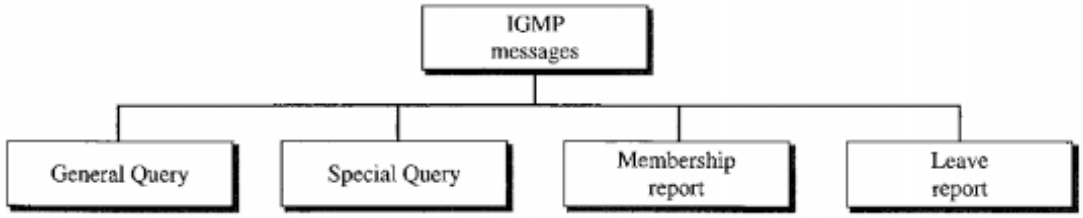
The Internet Group Management Protocol (IGMP) is one of the necessary, but not sufficient protocols that is involved in multicasting. Group Management For multicasting in the Internet we need routers that are able to route multicast packets. The routing tables of these routers must be updated by using one of the multicasting routing protocols.

IGMP is not a multicasting routing 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. The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network. IGMP is a group management protocol. It helps a multicast router create and update a list of loyal members related to each router interface.

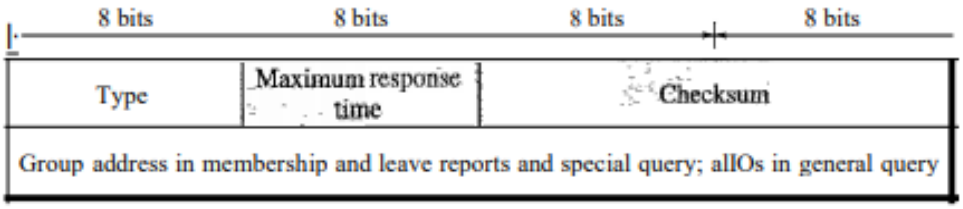
DOWNLOADED FROM KTUNOTES.IN

IGMP Messages:

IGMPv2 has three types of messages: the query, the membership report, and the leave report. There are two types of query messages: general and special.



Message Format:



Type. This 8-bit field defines the type of message, as shown in Table 21.1. The value of the type is shown in both hexadecimal and binary notation.

Table 21.1 *IGMP type field*

Type	*Value*
General or special query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave report	0x17 or 00010111

Maximum Response Time. This 8-bit field defines the amount of time in which a query must be answered. The value is in tenths of a second; for example, if the value is 100, it means 10 s. The value is nonzero in the query message; it is set to zero in the other two message types.

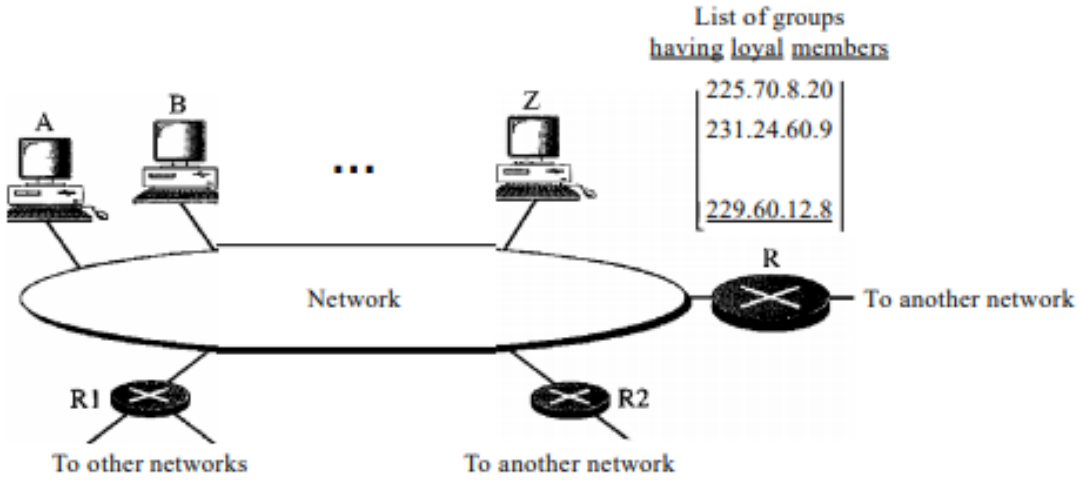
Checksum. This is a 16-bit field carrying the checksum. The checksum is calculated over the 8-byte message.

Group address. The value of this field is 0 for a general query message. The value defines the groupid (multicast address of the group) 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 with at least one loyal member in that network.

DOWNLOADED FROM KTUNOTES.IN



For each group, there is one router that has the duty of distributing the multicast packets destined for that group. This means that if there are three multicast routers connected to a network, their lists of groupids are mutually exclusive. For example, in 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 (an application program) receives multicast packets from some group. When a **router has membership**, it means that a network connected to one of its other interfaces receives these multicast packets. We say that the host or the router has **an interest in the group**. In both cases, the host and the router keep a list of groupids and relay their interest to the distributing router.

In the Figure, router R is the distributing router. There are two other multicast routers (R1 and R2) that, depending on the group list maintained by router R, could be the recipients of router R in this network. Routers RI and R2 may be distributors for some of these groups in other networks, but not on this network.

1. **Joining a Group**

A host or a router can join a group. A host maintains a list of processes that have membership in a group. When a process wants to join a new group, it sends its request to the host. The host adds the name of the process and the name of the requested group to its list. If this is the first entry for this particular group, the host sends a membership report message. If this is not the first entry, there is no need to send the membership report. The protocol requires that the membership **report be sent twice**, one after the other within a few moments. In this way, if the first one is lost or damaged, the second one replaces it.

2. **Leaving a Group**

When a host sees that no process is interested in a specific group, it sends a leave report. Similarly, when a router sees that none of the networks connected to its interfaces is interested in a specific group, it sends a leave report about that group. When a multicast router receives a leave report, The router allows a specified time for any host or router to respond. If, during this time, no interest (membership report) is received, the router assumes that there are no loyal members in the network and purges the group from its list.

DOWNLOADED FROM KTUNOTES.IN

3. Monitoring membership

There is only one host interested in a group, but the host is shut down or removed from the system. The multicast router will never receive a leave report. The multicast router is responsible for monitoring all the hosts or routers in a LAN to see if they want to continue their membership in a group. The router periodically (by default, every 125 s) sends a general query message. In this message, the group address field is set to 0.0.0.0. This means the query for membership continuation is for all groups in which a host is involved. The general query message does not define a particular group.

The query message has a maximum response time of 10. When a host or router receives the general query message, it responds with a membership report if it is interested in a group. However, if there is a common interest (two hosts, for example, are interested in the same group), only one response is sent for that group to prevent unnecessary traffic. This is called a **delayed response**. The query message must be sent by only one router called **the query router**, also to prevent unnecessary traffic.

4. Delayed Response

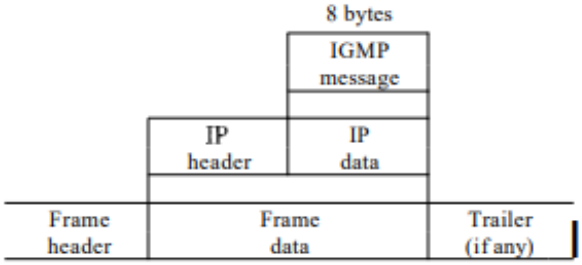
To prevent unnecessary traffic, IGMP uses a delayed response strategy. When a host or router receives a query message, it does not respond immediately; it delays the response. Each host or router uses a random number to create a timer, which expires between I and lOs. A timer is set for each group in the list. For example, the timer for the first group may expire in 2 s, but the timer for the third group may expire in 5 s. Each host or router waits until its timer has expired before sending a membership report message. During this waiting time, if the timer of another host or router, for the same group, expires earlier, that host or router sends a membership report. Because, the report is broadcast, the waiting host or router receives the report and knows that there is no need to send a duplicate report for this group; thus, the waiting station cancels its corresponding timer.

5. Query Router

Query messages may create a lot of responses. To prevent unnecessary traffic, IGMP designates one router as the query router for each network. Only this designated router sends the query message, and the other routers are passive.

Encapsulation

The IGMP message is encapsulated in an IP datagram, which is itself encapsulated in a frame.



Encapsulation at Network Layer

The value of the protocol field is 2 for the IGMP protocol. Every IP packet carrying this value in its protocol field has data delivered to the IGMP protocol. When the message is encapsulated in the IP datagram, the value of TTL must be 1. This is required because the domain of IGMP is the LAN. No IGMP message must travel beyond the LAN. A TTL value of 1 guarantees that the

DOWNLOADED FROM KTUNOTES.IN

message does not leave the LAN since this value is decremented to 0 by the next router and, consequently, the packet is discarded.

Encapsulation at Data Link Layer
At the network layer, the IGMP message is encapsulated in an IP packet and is treated as an IP packet. However, because the IP packet has a multicast IP address, the ARP protocol cannot find the corresponding MAC (physical) address to forward the packet at the data link layer. What happens next depends on whether the underlying data link layer supports physical multicast addresses.

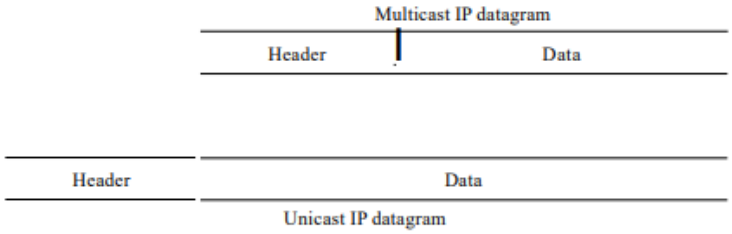
Physical Multicast Support Most LANs support physical multicast addressing. An Ethernet physical address (MAC address) is six octets (48 bits) long. If the first 25 bits in an Ethernet address identifies a physical multicast address for the TCP/IP protocol. The remaining 23 bits can be used to define a group. **To convert an IP multicast address into an Ethernet address**, the multicast router extracts the least significant 23 bits of a class D IP address and inserts them into a multicast Ethernet physical address.

An Ethernet multicast physical address is in the range 01 :00:5E:00:OO:OO to 01:00:5E:7F:FF:FF.

Change the multicast IP address 230.43.14.7 to an Ethernet multicast physical address.
Solution in two steps:
a. Write the rightmost 23 bits of the IP address in hexadecimal. This can be done by changing the rightmost 3 bytes to hexadecimal and then subtracting 8 from the leftmost digit if it is greater than or equal to 8. In our example, the result is 2B:OE:07.
b. We add the result of part a to the starting Ethernet multicast address, which is 01:00:5E:00:00:00. The result is 01:00:5E:2B:OE:07

Change the multicast IP address 238.212.24.9 to an Ethernet multicast address.
Solution
a. The rightmost 3 bytes in hexadecimal is D4: 18:09. We need to subtract 8 from the leftmost digit, resulting in 54:18:09.
b. We add the result of part a to the Ethernet multicast starting address. The result is 01:00:5E:54: 18:09

No Physical Multicast Support Most WANs do not support physical multicast addressing. To send a multicast packet through these networks, a process called **tunneling** is used. In tunneling, the multicast packet is encapsulated in a unicast packet and sent through the network, where it emerges from the other side as a multicast packet.



DOWNLOADED FROM KTUNOTES.IN

EXTERIOR ROUTING PROTOCOLS – BGP

Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. The Internet is divided into hierarchical domains called **autonomous systems.** Autonomous systems are divided into three categories: stub, multihomed, and transit.

Stub AS.
A stub AS has only one connection to another AS. The interdomain data traffic in a stub AS can be either created or terminated in the AS. The hosts in the AS can send data traffic to other ASs. The hosts in the AS can receive data coming from hosts in other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS is either a source or a sink. A good example of a stub AS is a small corporation or a small local ISP.

Multihomed AS.
A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.

Transit AS.
A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

Ktunotes.in

Attributes are divided into two broad categories: well known and optional. **A well-known** attribute is one that every BGP router must recognize. An **optional attribute** is one that needs not be recognized by every router.

Well-known attributes are themselves divided into two categories: mandatory and discretionary. **A well-known mandatory attribute** is one that must appear in the description of a route. A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message.
Examples:
ORIGIN. This defines the source of the routing information (RIP, OSPF, and so on).
AS_PATH. This defines the list of autonomous systems through which the destination can be reached.
NEXT-HOP, which defines the next router to which the data packet should be sent.

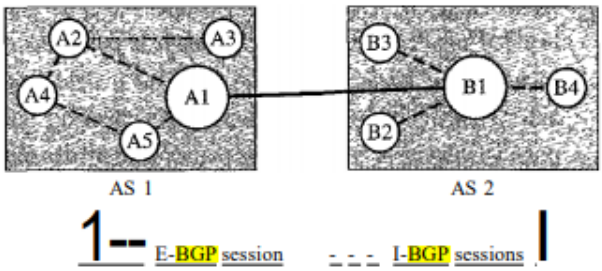
The optional attributes can also be subdivided into two categories: transitive and nontransitive. An **optional transitive attribute** is one that must be passed to the next router by the router that has not implemented this attribute.
An **optional nontransitive attribute** is one that must be discarded if the receiving router has not implemented it.

BGP Sessions
The exchange of routing information between two routers using BGP takes place in a session. A session is a connection that is established between two BGP routers only for the sake of

DOWNLOADED FROM KTUNOTES.IN

exchanging routing information. To create a reliable environment, BGP uses the services of TCP. For this reason, BGP sessions are sometimes referred to as **semi-permanent connections**.

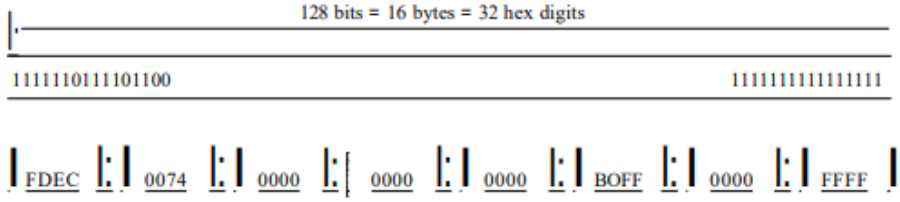
BGP can have two types of sessions: **external BGP (E-BGP)** and **internal BGP (I-BGP)** sessions.
The **E-BGP session** is used to exchange information between two speaker nodes belonging to two different autonomous systems.
The **I-BGP session**, on the other hand, is used to exchange routing information between two routers inside an autonomous systems.



IPV6 – ADDRESSING – ISSUES

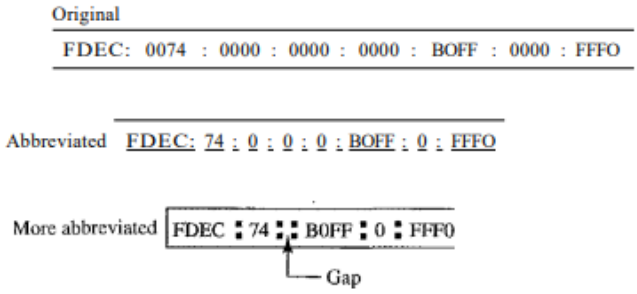
An IPv6 address consists of 16 bytes (octets); it is 128 bits long. IPv6 specifies hexadecimal colon notation. In this notation, 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

Figure 19.14 *IPv6 address in binary and hexadecimal colon notation*



Although the IP address, even in hexadecimal format, is very long, many of the digits are zer9s. In this case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted. Only the leading zeros can be dropped, not the trailing zeros.

Figure 19.15 *Abbreviated IPv6 addresses*



DOWNLOADED FROM KTUNOTES.IN

0074 can be written as 74, OOOF as F, and 0000 as O. We can remove the zeros altogether and replace them with a double semicolon. Note that this type of abbreviation is allowed only once per address. If there are two runs of zero sections, only one of them can be abbreviated.

Expand the address 0:15::1:12:1213 to its original.

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 0:   15:                      1:   12:1213
```

This means that the original address is

0000:0015:0000:0000:0000:0001 :0012:1213

Address Space

IPv6 has 2^{128} addresses available. IPv6 divided the address into several categories. A few leftmost bits, called **the type prefix**, in each address define its category. The type prefix is variable in length, but it is designed such that no code is identical to the first part of any other code. In this way, there is no ambiguity; when an address is given, the type prefix can easily be determined.

Table 19.5 *Type prefixes for IPv6 addresses*

Type Prefix	*Type*	*Fraction*
00000000	Reserved	1/256
00000001	Unassigned	1/256
0000001	ISO network addresses	1/128
0000010	IPX (Novell) network addresses	1/128
0000011	Unassigned	1/128
00001	Unassigned	1/32
0001	Reserved	*1/16*
001	Reserved	1/8
010	Provider-based unicast addresses	*1/8*

Table 19.5 *Type prefixes for IPv6 addresses (continued)*

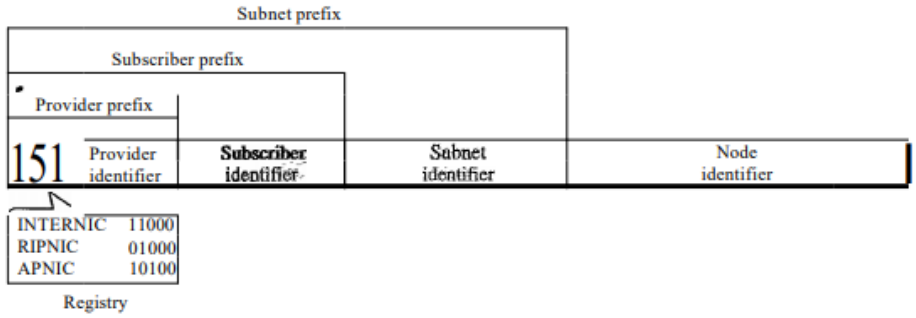
Type Prefix	*Type*	*Fraction*
011	Unassigned	1/8
100	Geographic-based unicast addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1116
11110	Unassigned	1132
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
11111110 a	Unassigned	1/512
1111 111010	Link local addresses	111024
1111 1110 11	Site local addresses	1/1024
11111111	Multicast addresses	1/256

DOWNLOADED FROM KTUNOTES.IN

Unicast Addresses

A unicast address defines a single computer. The packet sent to a unicast address must be delivered to that specific computer. IPv6 defines two types of unicast addresses: **geographically based** and **provider-based**. The provider-based address is generally used by a normal host as a unicast address.

Figure 19.16 *Prefixes for provider-based unicast address*

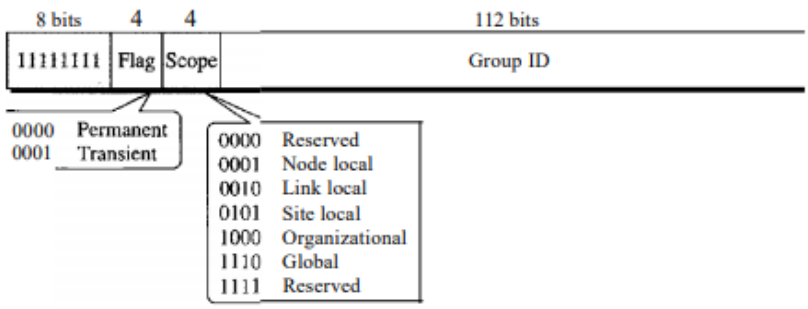


Type identifier. This 3-bit field defines the address as a provider-based address.
Registry identifier. This 5-bit field indicates the agency that has registered the address.
Provider identifier. This variable-length field identifies the provider for Internet access (such as an ISP). A 16-bit length is recommended for this field.
Subscriber identifier. When an organization subscribes to the Internet through a provider, it is assigned a subscriber identification. A 24-bit length is recommended for this field.
Subnet identifier. Each subscriber can have many different subnetworks, and each subnetwork can have an identifier. The subnet identifier defines a specific subnetwork under the territory of the subscriber. A 32-bit length is recommended for this field.
Node identifier. The last field defines the identity of the node connected to a subnet. A length of 48 bits is recommended for this field to make it compatible with the 48-bit link (physical) address used by Ethernet. In the future, this link address will probably be the same as the node physical address.

Multicast Addresses

Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group.

Figure 19.17 *Multicast address in IPv6*



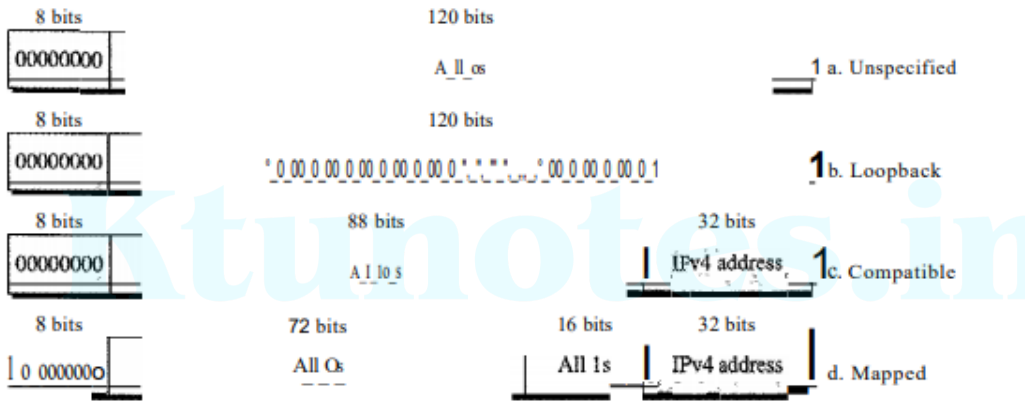
DOWNLOADED FROM KTUNOTES.IN

A flag that defines the group address as either permanent or transient. A **permanent group** address is defined by the Internet authorities and can be accessed at all times. A **transient group** address, on the other hand, is used only temporarily. Systems engaged in a teleconference, for example, can use a transient group address.
The third field defines **the scope** of the group address. Many different scopes are provided.

Anycast addresses.
An anycast address, like a multicast address, also defines a group of nodes. However, a packet destined for an anycast address is delivered to only one ofthe members ofthe anycast group, the nearest one (the one with the shortest route)

Reserved Addresses
These addresses start with eight Os (type prefix is 00000000). A few subcategories are defined in this category, as shown in Figure 19.18.

Figure 19.18 *Reserved addresses in IPv6*

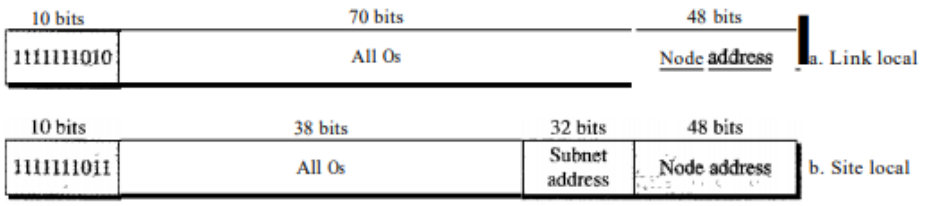


An unspecified address is used when a host does not know its own address and sends an inquiry to find its address.
A loopback address is used by a host to test itself without going into the network.
A compatible address is used during the transition from IPv4 to IPv6. It is used when a computer using IPv6 wants to send a message to another computer using IPv6, but the message needs to pass through a part of the network that still operates in IPv4.
A mapped address is also used during transition. However, it is used when a computer that has migrated to IPv6 wants to send a packet to a computer still using IPv4.

Local Addresses
These addresses are used when an organization wants to use IPv6 protocol without being connected to the global Internet. In other words, they provide addressing for private networks. Nobody outside the organization can send a message to the nodes using these addresses. Two types of addresses are defined for this purpose:

DOWNLOADED FROM KTUNOTES.IN

Figure 19.19 *Local addresses in IPv6*



A link local address is used in an isolated subnet; a site local address is used in an isolated site with several subnets.

Advantages

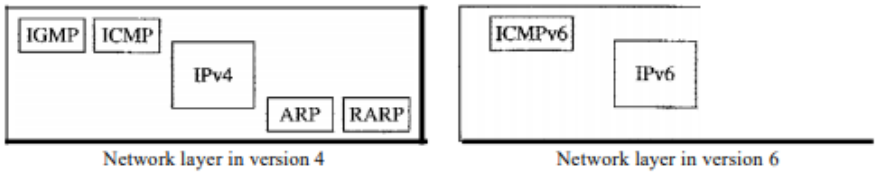
The next-generation IP, or IPv6, has some advantages over IPv4 that can be summarized as follows:

- Larger address space. An IPv6 address is 128 bits long, as we discussed in Chapter 19. Compared with the 32-bit address of IPv4, this is a huge (296) increase in the address space. O
- Better header format. IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- New options. IPv6 has new options to allow for additional functionalities.
- Allowance for extension. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- Support for resource allocation. In IPv6, the type-of-service field has been removed, but a mechanism (calledjlow label) has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

ICMPv6.

Comparison of the network layer of version 4 to version 6:

Figure 21.23 *Comparison ofnetwork layers in version* 4 *and version 6*



DOWNLOADED FROM KTUNOTES.IN

The ARP and IGMP protocols in version 4 are combined in ICMPv6. The RARP protocol is dropped from the suite because it was rarely used and BOOTP has the same functionality. Just as in ICMPv4, we divide the ICMP messages into two categories.

Error Reporting

As we saw in our discussion of version 4, one of the main responsibilities of ICMP is to report errors. Five types of errors are handled: destination unreachable, packet too big, time exceeded, parameter problems, and redirection. ICMPv6 forms an error packet, which is then encapsulated in an IP datagram. This is delivered to the original source of the failed datagram.

Table 21.3 *Comparison of error-reporting messages in ICMPv4 and ICMPv6*

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

The source-quench message is eliminated in version 6 because the priority and the flow label fields allow the router to control congestion and discard the least important messages. In this version, there is no need to inform the sender to slow down. The packet-too-big message is added because fragmentation is the responsibility of the sender in IPv6. Ifthe sender does not make the right packet size decision, the router has no choice but to drop the packet and send an error message to the sender.

- **Packet Too Big**

This is a new type of message added to version 6. If a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass, two things happen. First, the router discards the datagram and then an ICMP error packet-a packet-too-big message-is sent to the source.

Query

ICMP can diagnose some network problems. This is accomplished through the query messages. Four different groups of messages have been defined: echo request and reply, router solicitation and advertisement, neighbor solicitation and advertisement, and group membership.

Table 21.4 *Comparison of query messages in ICMPv4 and ICMPv6*

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address-mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

DOWNLOADED FROM KTUNOTES.IN

Two sets of query messages are eliminated from ICMPv6: time-stamp request and reply- and address-mask request and reply. The timestamp request and reply messages **are eliminated** because they are implemented in other protocols such as TCP and because they were rarely used in the past. The address-mask request and reply messages are eliminated in IPv6 because the subnet section of an address allows the subscriber to use up to 232 - 1 subnets. Therefore, subnet masking, as defined in IPv4, is not needed here.

Neighbor Solicitation and Advertisement

the network layer in version 4 contains an independent protocol called Address Resolution Protocol (ARP). In version 6, this protocol is eliminated, and its duties are included in ICMPv6. The idea is exactly the same, but the format of the message has changed.

Group Membership

The network layer in version 4 contains an independent protocol called IGMP. In version 6, this protocol is eliminated, and its duties are included in ICMPv6. The purpose is exactly the same.

Ktunotes.in

DOWNLOADED FROM KTUNOTES.IN