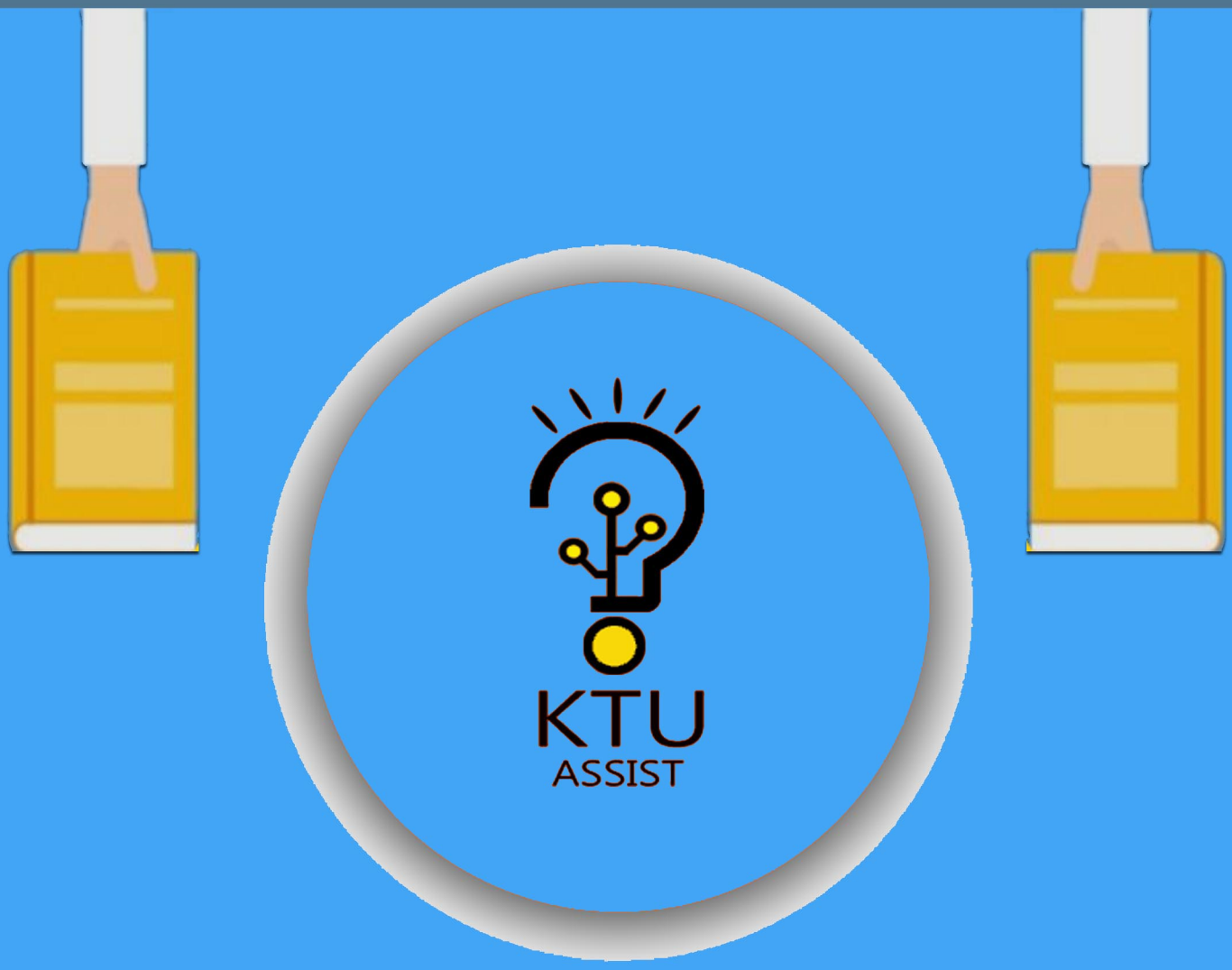
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

STUDY MATERIALS



Module 6

Transport and Application Layer & WWW

TRANSPORT LAYER

Ques 1) What is transport layer? What are the functions of transport layer?

Ans: Transport Layer
The transport layer is the fourth layer of the OSI reference model. Transport layer provides transparent, reliable, and cost effective transfer of data units between the upper layer entities in the end systems.

The goal of the transport layer is to abstract the structure and function of the network so that the upper layer can communicate without needing to consider the network technology.

Functions of Transport Layer
The basic functions of Transport Layer are:

1) **End-to-End Delivery:** The network layer oversees the end-to-end delivery of individual packets but does not see any relationship between those packets, even those belonging to a single message. It treats each as an independent entity.
2) **Addressing:** The client needs the address of the remote computer it wants to communicate with. Such remote computers have a unique address so that it can be distinguished from all the other computers.
3) **Reliable Delivery:** The reliable delivery considers the following issues given below:
   i) **Error Control:** When transferring data, the primary goal of reliability is error control. Data must be delivered to their destination exactly as they originated from the source. The realities of physical data transport are that, while 100 percent error-free delivery is probably impossible, transport layer protocols are designed to come as close as possible.
   ii) **Sequence Control:** The second aspect of reliability implemented at the transport layer is sequence control. On the sending end, the transport layer is responsible for ensuring that data units received from the upper layers are usable by the lower layers.

   On the receiving end, it is responsible for ensuring that the various pieces of a transmission are correctly reassembled.
   iii) **Loss Control:** The third aspect of reliability covered by the transport layer is loss control. The transport layer ensures that all pieces of a transmission arrive at the destination, not just some of them.
   iv) **Duplication Control:** The fourth aspect of reliability covered by the transport layer is duplication control. Transport layer functions must guarantee that no pieces of data arrive at the receiving system duplicated.
4) **Flow Control:** Fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information. The amount of memory on a computer is limited, and without flow control a larger computer might flood a computer with so much information that it can't hold it all before dealing with it.

   Nowadays, this is not a big issue, as memory is cheap while bandwidth is comparatively expensive, but in earlier times it was more important. Flow control allows the receiver to respond before it is overwhelmed.
5) **Multiplexing:** To improve transmission efficiency, the transport layer has the option of multiplexing.

Ques 2) What is TCP? Write the TCP packet format?

Ans: Transmission Control Protocol (TCP)
The Transmission Control Protocol (TCP) is a connection-oriented reliable protocol. It provides a reliable transport service between pairs of processes executing on End Systems (ES) using the network layer service provided by the IP protocol.

It is the general protocol suite of the Internet; encompassing protocols for network activities such as datagram delivery ad acknowledgement and protocols for user activity such as remote login (Telnet) and file transfer protocol (FTP). A given

implementation of TCP/IP application typically contains a dozen or more protocols and facilities essential to the use of TCP/IP application in a TCP/IP environment. It is a **two-layer** predominant transfer protocol that provides a reliable connection oriented, byte stream service.

A key feature of TCP, and one which dominates the protocol design, is that every byte on a TCP connection has its own 32-bit sequence number.

The sending and receiving TCP entities exchange data in the form of segments. A TCP segment consists of a fixed 20-byte header (plus an optional part) followed by zero or more data bytes. The TCP software decides how big segments should be. It can accumulate data from several writes into one segment or can split data from one write over multiple segments. Two limits restrict the segment size:

1) Each segment, including the TCP header, must fit in the 65515-byte IP payload.
2) Each network has a Maximum Transfer Unit, or MTU, and each segment must fit in the MTU. MTU is generally 1500 bytes (the Ethernet payload size) and thus defines the upper bound on segment size.

The basic protocol used by TCP entities is the sliding window protocol. When a sender transmits a segment, it also starts a timer. When the segment arrives at the destination, the receiving TCP entity sends back a segment (with data if any exist, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive. If the sender's timer goes-off before the acknowledgement is received, the sender transmits the segment again.

TCP Packet Format

The following descriptions summarise the TCP packet fields illustrated in **figure 6.1**:

1) **Source Port and Destination Port:** Identifies points at which upper-layer source and destination processes receive TCP services.
2) **Sequence Number:** Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.

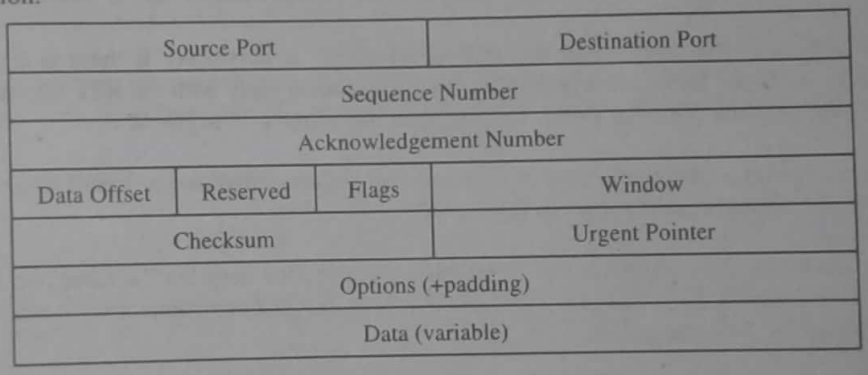


Figure 6.1: TCP Packet Format

3) **Acknowledgment Number:** Contains the sequence number of the next byte of data the sender of the packet expects to receive.
4) **Data Offset:** Indicates the number of 32-bit words in the TCP header.
5) **Reserved:** Remains reserved for future use.
6) **Flags (6 bits):** For each flag, if set to 1, the meaning is as follows:
   i) **CWR:** Congestion window reduced.
   ii) **ECE:** ECN-Echo; the CWR and ECE bits, defined in RFC 3168, are used for the explicit congestion notification function.
   iii) **URG:** Urgent pointer field significant.
   iv) **ACK:** Acknowledgment field significant.
   v) **PSH:** Push function.
   vi) **RST:** Reset the connection.
   vii) **SYN:** Synchronise the sequence numbers.
   viii) **FIN:** No more data from sender.
7) **Window:** Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).
8) **Checksum:** Indicates whether the header was damaged in transit.

9) **Urgent Pointer:** Points to the first urgent data byte in the packet.
10) **Options:** Specifies various TCP options.
11) **Data:** Contains upper-layer information.

Ques 3) Discuss how the connection is established and released in the TCP.

Ans: TCP Connection Establishment
To establish a connection, one side, say, the server passively waits for an incoming connection by executing the LISTEN and ACCEPTS primitives, either specifying a specific source or nobody in particular. The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password). The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit-off and waits for a response.

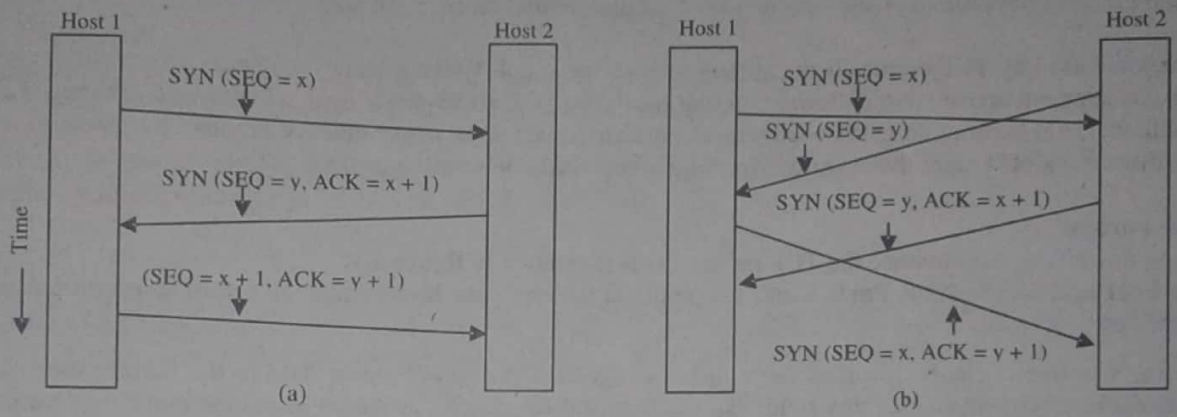


Figure 6.2: (a) TCP Connection Establishment in the Normal Case (b) Call Collision

When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the Destination port field. If not, it sends a reply with the RST bit onto reject the connection. If some process is listening to the port, that process is given the incoming TCP segment.

It can then either accept or reject the connection. If it accepts, an acknowledgement segment is sent back. The sequence of TCP segments sent in the normal case is shown in **figure 6.2**.

In the event that two hosts simultaneously attempt to establish a connection between the same two sockets, the sequence of events is as illustrated in **figure 6.2(b)**. The result of these events is that just one connection is established, not two because connections are identified by their end points.

TCP Connection Release
TCP connections are full duplex, now connections are released, it is best to think of them as a pair of simplex connections. Each simplex connection is released independently of its sibling.

To release a connection, either party can send a TCP segment with the FIN bit set, which means that it has no more data to transmit. When the FIN is acknowledged, that direction is shut-down for new data.

Data may continue to flow indefinitely in the other direction, however. When both directions have been shut down, the connection is released. Normally, four TCP segments are needed to release a connection, one FIN and one ACK for each direction. However, it is possible for the first ACK and the second FIN to be contained in the same segment, reducing the total count to three.

To avoid the two-army problem, timers are used. If a response to a FIN is not forthcoming within two maximum packet lifetimes, the sender of the FIN releases the connection.

Ques 4) Discuss about the TCP transmission policy.

Ans: TCP Transmission Policy
Window management in TCP is not directly tied to acknowledgements as it is in most data link protocols. **For example,** suppose the receiver has a 4096-byte buffer, as shown in **figure 6.3**. If the sender transmits a 2048-byte segment that is correctly received, the receiver will acknowledge the segment.

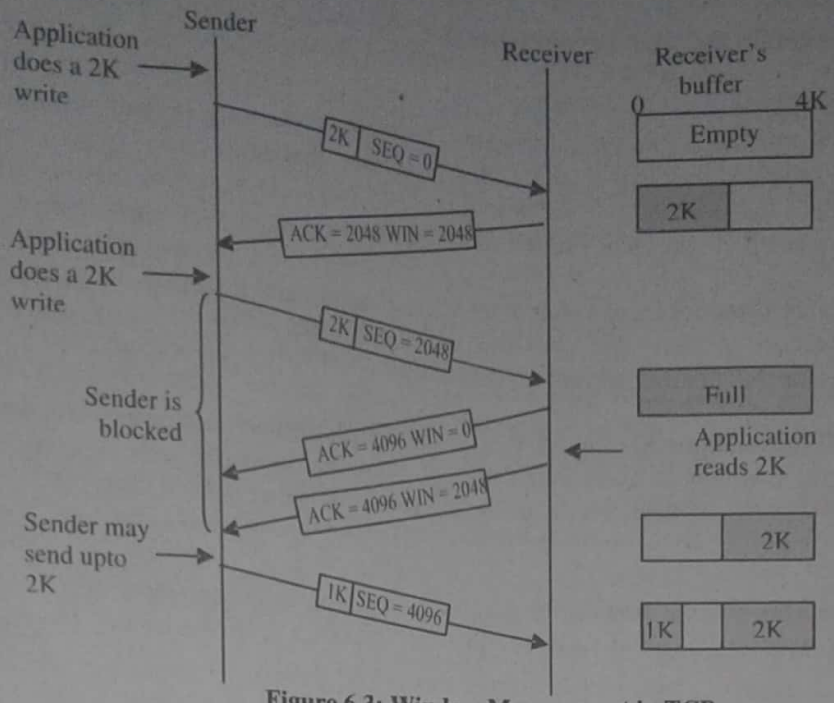


Figure 6.3: Window Management in TCP

However, since now it has only 2048 bytes of buffer space (until the application removes some data from the buffer), it will advertise a window of 2048 starting at the next byte expected.

Now the sender transmits another 2048 bytes, which are acknowledged, but the advertised window is 0. The sender must stop until the application process on the receiving host has removed some data from the buffer, at which time TCP can advertise a larger window. When the window is 0, the sender may not normally send segments, with two exceptions:

1) Urgent data may be sent, e.g., to allow the user to kill the process running on the remote machine.
2) The sender may send a 1-byte segment to make the receiver re-announce the next byte expected and window size. The TCP standard explicitly provides this option to prevent deadlock if a window announcement ever gets lost.

Ques 5) What are the different TCP services?

Ans: TCP Services

There is a long list of services that can be optionally provided by the Transport Layer. All available services are:

1) **Connection-Oriented:** This is normally easier to deal with than connection-less models, so where the Network layer only provides a connection-less service, often a connection-oriented service is built on top of that in the Transport Layer.

2) **Reliable Data:** Packets may be lost in routers, switches, bridges and hosts due to network congestion, when the packet queues are filled and the network nodes have to delete packets. Packets may be lost or corrupted in Ethernet due to interference and noise, since Ethernet does not retransmit corrupted packets. Packets may be delivered in the wrong order by an underlying network.

   By means of an error detection code, **for example** a checksum, the transport protocol may check that the data is not corrupted, and verify that by sending an ACK message to the sender. Automatic repeat request schemes may be used to retransmit lost or corrupted data.

3) **Flow Control:** The amount of memory on a computer is limited, and without flow control a larger computer might flood a computer with so much information that it can't hold it all before dealing with it. Flow control allows the receiver to respond before it is overwhelmed.

4) **Congestion Avoidance:** Network congestion occurs when a queue buffer of a network node is full and starts to drop packets. Automatic repeat request may keep the network in a congested state. This situation can be avoided by adding congestion avoidance to the flow control, including slow-start.

5) **Byte Orientation:** The Transport Layer may add the ability to view communication just as a stream of bytes. This is nicer to deal with than random packet sizes, however, it rarely matches the communication model which will normally be a sequence of messages of user defined sizes.

6) **Ports:** Ports are essentially ways to address multiple entities in the same location. **For example,** the first line of a postal address is a kind of port, and distinguishes between different occupants of the same house.

Ques 6) What is UDP? Also explain the UDP header format.

Ans: User Datagram Protocol (UDP)
User Datagram Protocol (UDP) provides a minimal, unreliable, best-effort, message-passing transport to applications and upper-layer protocols. Service provided by UDP is an unreliable service that provides no guarantees for delivery and no protection from duplication (e.g. if this arises due to software errors within an Intermediate System (IS)). The simplicity of UDP reduces the overhead from using the protocol and the services may be adequate in many cases.

UDP communication consequently does not incur connection establishment and teardown overheads and there is minimal associated end system state. Because of these characteristics, UDP can offer a very efficient communication transport to some applications, but has no inherent congestion control or reliability.

A unique characteristic of UDP is that it provides no inherent on many platforms, applications can send UDP datagrams at the line rate of the link interface, which is often much greater than the available path capacity and doing so would contribute to congestion along the path, applications therefore need to be designed responsibly.

UDP Header Format
A computer may send UDP packets without first establishing a connection to the recipient. The computer completes the appropriate fields in the UDP header (PCI) and forwards the data together with the header for transmission by the IP network layer.

Figure 6.4 shows that the UDP protocol header consists of 8 bytes of Protocol Control Information (PCI).

Bits	0-15	16-31
0	Source port	Destination port
32	Length	Checksum
64	Data	

Figure 6.4: Header Format of UDP

The UDP header consists of four fields each of 2 bytes in length:

1) **Source Port:** UDP packets from a client use this as a service access point (SAP) to indicate the session on the local client that originated the packet. UDP packets from a server carry the server SAP in this field.
2) **Destination Port:** UDP packets from a client use this as a service access point (SAP) to indicate the service required from the remote server. UDP packets from a server carry the client SAP in this field.
3) **UDP Length:** The number of bytes comprising the combined UDP header information and payload data.
4) **UDP Checksum:** A checksum to verify that the end to end data has not been corrupted by routers or bridges in the network or by the processing in an end system. The algorithm to compute the checksum is the Standard Internet Checksum algorithm. If this check is not required, the value of 0x0000 is placed in this field, in which case the data is not checked by the receiver.

Ques 7) Explain the different operations performed by UDP.

Ans: UDP Operations
The operations performed by UDP are as below:

1) **Connectionless Service**
   i) This means that each user datagram sent by UDP is an independent datagram i.e., no relationship between the user datagrams even if they belong to the same destination program.
   ii) The user datagrams are not numbered; there is no connection establishment and no connection release.
   iii) This means that each user datagram can travel on a different path.
   iv) A process using UDP cannot send a stream of data. Each request should be small enough to fit into one user datagram. Only those processes sending short messages should use UDP.

2) **Flow and Error Control**
   i) There is no flow control. The receiver may then overflow.
   ii) There is no error control except for the checksum. The sender could not know if the message has been lost or duplicated. The receiver silently discards a user datagram when an error is detected by the checksum.
   iii) The process using UDP should provide the flow and error control if they are needed.
   iv) No connection state (sequence and ACK numbers, send and receive buffers? etc.) is needed.

3) **Encapsulation and Decapsulation:** To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram. In UDP, queues are associated with ports. At the client site, when a process starts, it requests a port number from the operating system. Some implementations create both an incoming and an outgoing queue associated with each process. Other implementations create only an incoming queue associated with each process.

Even if a process wants to communicate with multiple processes, it obtains only one port number and eventually one outgoing and one incoming queue. The queues opened by the client are, in most cases, identified by ephemeral port numbers. The queues function as long as the process is running. When the process terminates, the queues are destroyed.

The client process can send messages to the outgoing queue by using the source port number specified in the request. UDP removes the messages one by one and, after adding the UDP header, delivers them to IP. An outgoing queue can overflow. If this happens, the operating system can ask the client process to wait before sending any more messages.

When a message arrives for a 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.

4) **Queuing:** In UDP, queues are associated with ports.
   i) **At Client Site**
      a) When a process starts, it requests a port number from the OS.
      b) Some implementations create both incoming and outgoing queue associated with each process. Other implementations create only an incoming queue.
      c) These queues are identified by the ephemeral port numbers assigned. These queues function as long as the process is running. They are destroyed when the process terminates.
      d) The client process can send messages to the outgoing queue by using the source port number specified in the request.
      e) An outgoing queue can overflow. The OS asks then the client to wait before sending any more messages.
      f) When a message arrives for a client, UDP checks if an incoming queue has been created for the port number specified in the destination port. If so, UDP sends the received user datagram to the end of the queue. Otherwise, UDP discards the user datagram and asks ICMP to send a port unreachable message to the server.
      g) An incoming queue can overflow. UDP drops then the user datagram and asks for a port unreachable message to be sent to the server.

   ii) **At Server Site**
      a) The mechanism of creating queues is different.
      b) The server asks for incoming and outgoing queues, using its well-known ports, when it starts. These queues remain open as long as the server is running.
      c) When a message arrives to the server, UDP checks to if an incoming queue has been created for the port number specified in the destination port number.
      If so, UDP places the user datagram at the end of the queue. Otherwise, UDP discards the user datagram and asks ICMP to send an unreachable port message to the client.
      d) An incoming queue can overflow. UDP drops the user datagram and asks that a port unreachable message to be sent to the client.
      e) When a server wants to respond to a client, it sends messages to the outgoing queue using the source port number specified in the request. UDP encapsulates the user datagram get from the outgoing queue in IP packets.
      f) If the outgoing queue overflows, the OS asks the server to wait before sending any more messages.

Ques 8) What is difference between UDP and TCP?

Ans: Comparison between UDP and TCP

Table 6.1 shows the major difference between UDP and TCP protocols.

Table 6.1: Comparison between UDP and TCP

Characteristics	UDP	TCP
General Description	Simple, high speed, low functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliable without worrying about network layer issues.
Data Interface to Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.

Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
Retransmission	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Managing flow of data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low ,but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quality	Small to moderate amounts of data(up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Protocol Connection Setup	Connections less; details sent without setup.	Connection-oriented; connection must be established prior to transmission.
Applications and Protocols	Multimedia applications, DNS,BOOTP,DHCP,TFTP, SNMP,RIP,NFS	FTP, Telnet, SMTP, DNS,HTTP POP,NNTP,IMAP,BGP, IRC,NFS

APPLICATION LAYER

Ques 9) What is application layer? What are the functions of application layers?

Ans: Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model.

The application layer programs are based on client and servers.

Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication:

1) When **identifying communication partners**, the application layer determines the identity and availability of communication partners for an application with data to transmit.
2) When **determining resource availability**, the application layer must decide whether sufficient network resources for the requested communication exist.
3) In **synchronizing communication**, all communication between applications requires cooperation that is managed by the application layer.

Some **examples** of application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Functions of Application Layers

1) **File Transfer, Access, and Management (FTAM):** This application allows a user to access files in a remote computer (to make changes or read data), to retrieve files from a remote computer; and to manage or control files in a remote computer. FTAM enables users to:
   i) Access file stores both locally and remotely, make FTAM a distributed file access protocol more similar to Gopher in this regard than to FTP.
   ii) Integrate management of both local and remote file stores, including the ability to manipulate both files and their attributes.
   iii) Access files stores on different kinds of machines that have different types of file systems.
   iv) Transfer files both synchronously and asynchronously.

   FTAM model defines the architecture of a hierarchical virtual file store in terms of file structure, file attributes, and the kinds of operations that can be performed on files and their attributes.
2) **Addressing:** For communication between client and server there is requirement of address. When the client request is made to server, it also contains server address and its own address. The server response also contains destination address, i.e., the address of the client. DNS is used for this addressing.

3) **Mail Services:** This application provides the basis for e-mail forwarding and storage.
4) **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.
5) **Authentication:** Authenticates the sender or receiver of the message or both.

Ques 10) What is the File Transfer Protocol (FTP)? What are the objectives of FTP?
Or
Discuss about the mechanism of FTP.

Ans: File Transfer Protocol (FTP)
FTP allows the transfer of files from one computer to another. File can be in any format like text, graphics, sound, etc. It activates the client-server relationship. Thus, whatever that can be stored in a computer can be moved with the FTP service.

Objectives of FTP
1) Its main objective is to help in sharing of programs and data.
2) Inspiring the implicit use of remote computers is another objective of FTP.
3) To protect the user from variation in file storage systems among numerous hosts.
4) Effective and reliable sharing of data.

Mechanism of FTP
The fundamental model of FTP is shown in **figure 6.5**. In this model a client has following three components:
1) User Interface,
2) Client Control Process, and
3) Client Data Transfer Process.

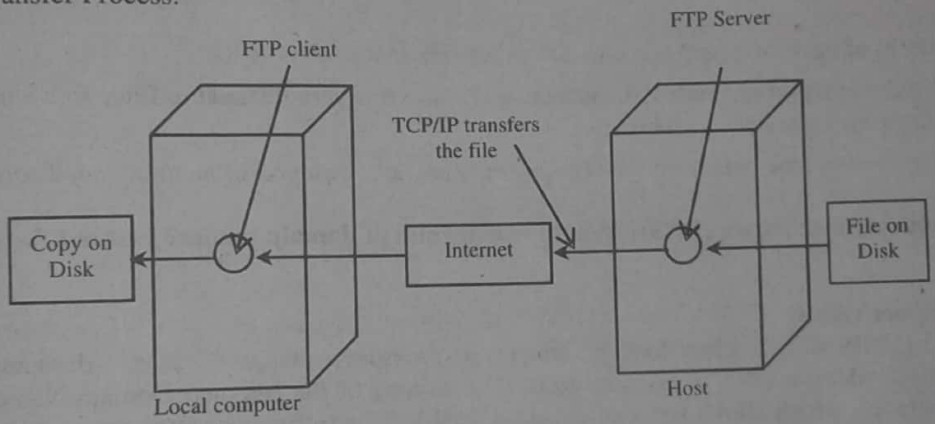


Figure 6.5: Mechanism of FTP

In the FTP model, server has two basic components:
1) Server Control Process and
2) Server Data Transfer Process

Figure 6.5 shows the mechanism of FTP. Its process of transferring a file is as follows:
1) First, define the address of remote computer on your computer as a parameter.
2) Then run the FTP command on your computer known as 'FTP client process', which makes a connection with the FTP process running on remote computer known as 'FTP server process'.
3) After running the FTP command user needs to enter the username and password to ensure that user is authorised to access the remote computer.
4) On successful login, the user is able to download or upload files using 'get' and 'put' commands. Listing of directories and navigating between directories before any transferred decision can also be done.

FTP has two connections:
1) **Control Connection:** This is a control process connection. During the complete FTP session, control connections remain connected.
2) **Data Connection:** This connection is present between various data transfer processes. During every file transfer, this connection opens and after completion of 'transfer process', this connection gets closed.

These connections use different techniques and port numbers.

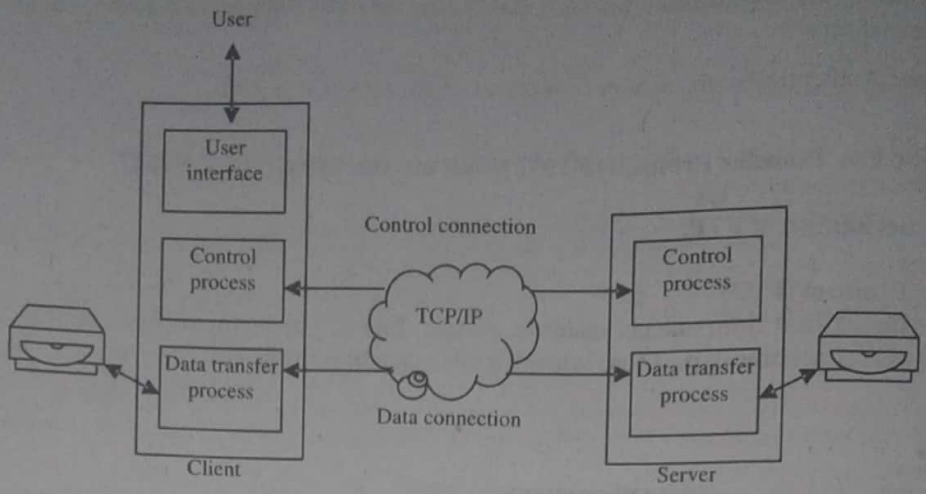


Figure 6.6: FTP

Ques 11) What are the advantages and disadvantages of FTP?

Ans: Advantages of FTP

1) It is the fastest and efficient method to receive (or download) big files from a computer to another computer.
2) It is more secure because user cannot transfer and get the files and directories without login (every FTP server requires a username and password to login).

Disadvantages of FTP

1) There are possibilities of eavesdropping because all the data are sent in clear text.
2) User always uses a random port to create the connection because it is very difficult to filter active mode FTP traffic by using firewall at the user's end (local machine).
3) There is a possibility to send the data from remote system to any arbitrary port of an unintended computer.

Ques 12) What is Domain Name Space (DNS)? What is the format of domain names? List out the different elements of DNS.

Ans: Domain Name Space (DNS)

Domain Name System (DNS) is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address. DNS is essential to the functioning of the Internet. Domain Name System (DNS) is service on a TCP/IP network which allows users of networks to utilise user-friendly names when looking for other hosts (i.e., computers) instead of having to remember and use their IP Addresses. This system is used extensively on die Internet and in many private enterprises today.

For example, suppose the FTP site at **EduSoft** had an IP Address of 132.147.165.50, most people would reach this computer by specifying ftp.EduSoft.com and not the less user-friendly IP Address. Besides being easier to remember, the name is more reliable. The numeric address could change for any number or reasons, but the name can always be used.

Format of Domain Names

Figure 6.7 shows a basic format of the domain name:

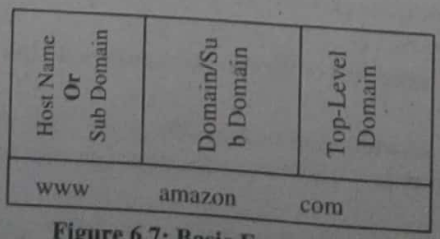


Figure 6.7: Basic Format of Domain Name

The exact layout may vary because sometimes an address may have some more parts. Domain is divided into many subdomains. Sometimes a domain name has the second and top-level domain such as 'www.tppl.co.in' where '.co' is the second level domain and '.in' is the top-level domain.

Elements of DNS

Four elements comprise the DNS are:

1) DNS Name Space
2) DNS Database
3) Name Servers
4) DNS Resolvers

Ques 13) What do you understand by DNS name space?

Ans: DNS Name Space

There are hundreds of top-level domains which categorise the Internet and every domain has many hosts. These domains are divided into various sub-domains, which are further divided into various other levels and so on.

Figure 6.8 shows the tree structure of domains. In this figure, leaves domains have no sub-domain but may include single host (node) or may represent even an organisation having thousands of other hosts (nodes).

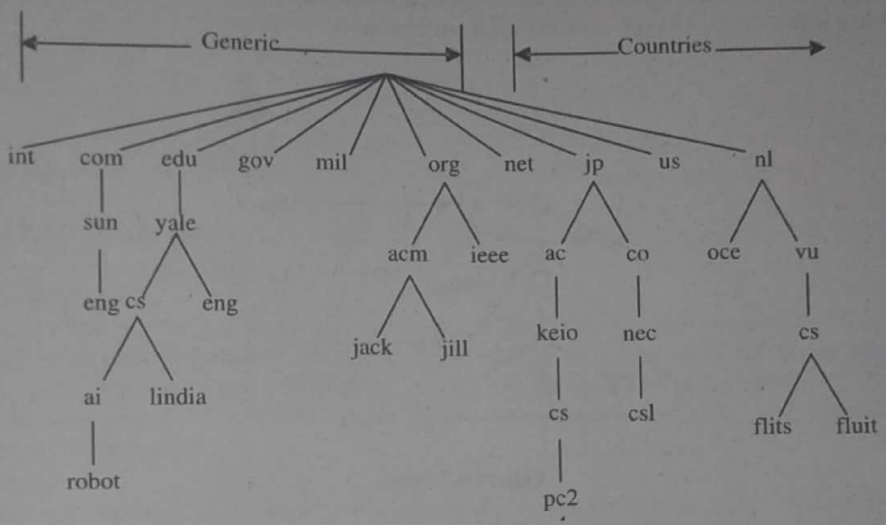


Figure 6.8 A Portion of the Internet Domain Name Space

The leaves of the tree represent domains that have no subdomains (but do contain machines, of course) A leaf domain may contain a single host, or it may represent a company and contains thousands of hosts.

The top-level domains come in two flavours: and **countries**:

1) **Generic:** The generic domains are:
   i) com (commercial)
   ii) edu (educational institutions),
   iii) gov (the U.S. federal government),
   iv) int (certain international organisations),
   v) mil (the U.S. armed forces),
   vi) net (network providers), and
   vii) org (nonprofit organisations).
2) **Country:** The country domains include one entry for every country, as defined in ISO 3166. Each domain is named by the path upward from it to the (unnamed) root. The components are separated by periods (pronounced "dot"). **For example,** Sun Microsystems engineering department might be eng.sun.com.

Domain names can be either **absolute** or **relative**:

1) **Absolute:** An absolute domain name ends with a period (e.g., eng.sun.com.).
2) **Relative:** Relative names have to be interpreted in some context to uniquely determine their true meaning. , It does not end with a dot period.

In both cases, a named domain refers to a specific node in the tree and all the nodes under it.

Domain names are case insensitive, so edu and EDU mean the same thing. Component names can be up to 63 characters long, and full path names must not exceed 255 characters.

Ques 14) What is zone?

Ans: Zone
A zone is a contiguous portion of the domain namespace for which a DNS server has the authority to resolve DNS queries. The namespace can be divided up into zones, which store name information about one or more DNS domains or portions of a domain.

A zone is the authoritative source for information about each domain name included in that zone. One can configure a single DNS server to host multiple zones, but conversely, can also configure multiple servers to host one or more zones to provide fault tolerance and distribute name resolution and administrative workload.

Multiple zones in a domain name space can be used to distribute administrative tasks to different groups. However, a zone must encompass a contiguous domain name space.

One cannot create a zone that consists of only of admin.coatbank.com and finance.coatbank.com because these two domains are not contiguous - the admin and finance subdomains are independent of each other and can only be combined into a single DNS zone if the coatbank.com domain is also included in the zone.

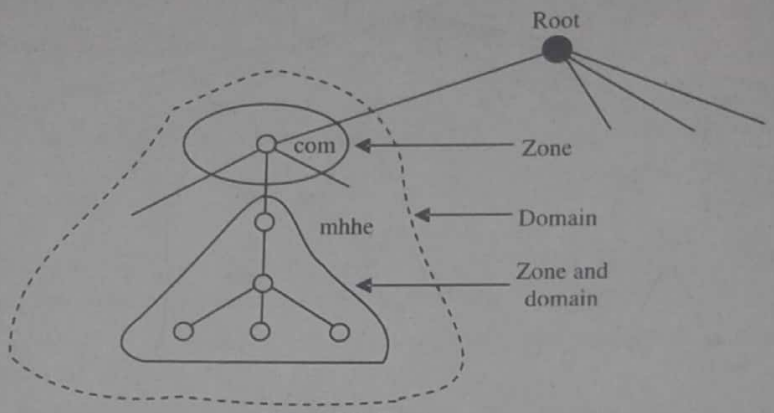


Figure 6.9: Zone

Zone files contain information that a DNS server references to resolve host names to IP addresses and to resolve IP addresses to host names. This information is stored as resource records that populate the zone file.

A zone file contains the name resolution data for a zone, including resource records that contain information for answering DNS queries. Resource records are database entries that contain various attributes of a computer, such as the host name or FQDN, the IP address, or the alias. DNS servers can contain various types of resource records.

Ques 15) What is domain resource record?

Ans: Domain Resource Records
DNS does not only deal with IP-addresses of hosts, but also exchanges information on name servers. There are in fact a whole bunch of different types of entries that a DNS database may have.

The key features of the database are as follows:

1) **Variable-Depth Hierarchy for Names:** DNS allows essentially unlimited levels and uses the period (.) as the level delimiter in printed names.
2) **Distributed Database:** The database resides in DNS servers scattered throughout the Internet and private intranets.
3) **Distribution Controlled by Database:** The DNS database is divided into thousands of separately managed zones, which are managed by separate administrators. The database software controls distribution and update of records.

A single piece of information from the DNS database is called a resource record (RR). DNS is based on a hierarchical database containing resource records (RRs) that include the name, IP address, and other information about hosts. A resource record is a five-tuples are encoded in binary for efficiency, in most expositions resource records are presented as ASCII text, one line per resource record.

Syntax:

Domain_name Time_to_live Class Type Value

Where,

1) **Domain_name Field:** It tells the domain to which this record applies.
2) **Time_to_live Field:** This field gives an indication of how stable the record is.
3) **Class Field:** For Internet information, it is always IN. For non-internet information, other codes can be used, but in practice, these are rarely seen.
4) **Type Field:** This field tells what kind of record this is. The most important types are listed in **table 6.2.**

Table 6.2: Principle DNS Resource Record Types

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

5) **Value Field:** This field can be a number, a domain name or an ASCII string. The semantic depend on the record type. A short description of the Value fields for each of the principal records types is given in **table 5.1.**

Ques 16) What are the domain name servers?

Ans: Domain Name Servers

In theory at least, a single name server could contain the entire DNS database and respond to all queries about it. In practice, this server would be so overloaded as to be useless. Furthermore, if it ever went down, the entire Internet would be crippled. To avoid the problems associated with having only a single source of information, the DNS name space is divided up into non-overlapping zones. Each zone contains some part of the tree and also contains name servers holding the authoritative information about that zone.

Normally, a zone will have one primary name server, which gets its information from a file on its disk, and one or more secondary name servers, which get their information from the primary name server.

To improve reliability, some servers for a zone can be located outside the zone. **For example,** in **figure 5.2** part of the DNS name space showing the division into zones, Yale has a server for yale.edu that handles eng.yale.edu but not cs.yale.edu, which is a separate zone with its own name servers.

Such a decision might be made when a department such as English does not wish to run its own name server, but a department such as computer science does. Consequently, cs.yale.edu is a separate zone but eng.yale.edu is not.

Where the zone boundaries are placed within a zone is up to that zone's administrator. This decision is made in large part based on how many name servers are desired, and where.

Ques 17) What is DNS Resolver? Also discuss about the recursive and iterative query.

Or

Explain about the address resolution mechanism.

Ans: DNS Resolvers

The client-side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought, e.g., translation of a domain name into an IP address.

DNS clients are configured with the addresses of DNS servers. Usually, these are servers which are authoritative for the domain of which they are a member. All requests for name resolution start with a request to one of these local servers.

DNS queries can be of two forms:

1) **Recursive Query:** A recursive query asks the nameserver to resolve a name completely, and return the result. If the request cannot be satisfied directly, the nameserver looks in its configuration and caches for a server higher up the domain tree which may have more information.

In the worst case, this will be a list of pre-configured servers for the root domain. These addresses are returned in a response called a referral. The local nameserver must then send its request to one of these servers.

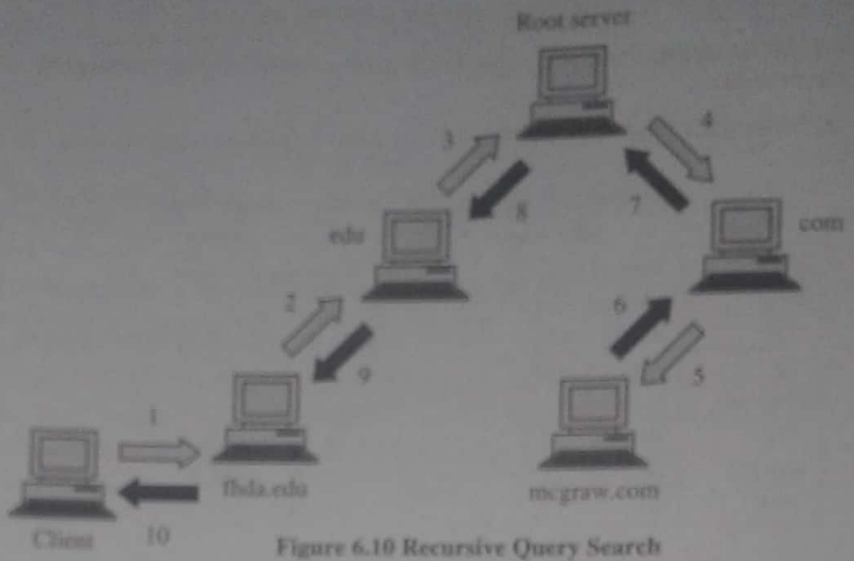


Figure 6.10 Recursive Query Search

2) **Iterative Query:** It asks the second nameserver to either respond with an authoritative reply, or with the addresses of nameservers (NS records) listed in its tables or caches as authoritative for the relevant zone. The local nameserver then makes iterative queries, walking the tree downwards until an authoritative answer is found (either positive or negative) and returned to the client.

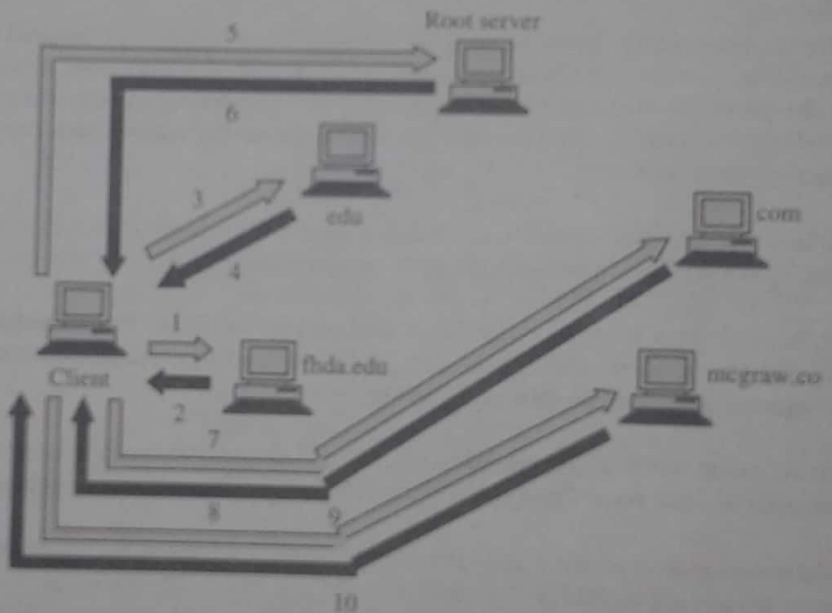


Figure 6.11 Iterative Query Search

In order to resolve the IP address of a domain name, a name server works on the domain name segment by segment, from highest-level domain appearing on the right, to lowest-level domain on the left. The resolver usually has to query several servers that are authoritative for various portions of the domain name to find all the necessary information.

A name server begins a search by first checking its own name space. If the queried domain name is not part of its space, the name server then issues a query to a root name server. A name server begins a search by first checking its own name space. If the queried domain name is not part of its space, the name server then issues a query to a root name server. In theory a full host name may have several name segments, (e.g., ahost.ofasubnet.ofabiggernet.inadomain.example).

In practice, full host names will frequently consist of just three segments (ahost.inadomain.example and most often www.inadomain.example).

For querying purposes, software interprets the name segment by segment, from right to left. At each step along the way, the program queries a corresponding DNS server to provide a pointer to the next server which it should consult. A DNS recursor consults three nameservers to resolve the address www.thakur.org.

Process: Address Resolution Mechanism

Step 1: The local system is pre-configured with the known addresses of the root servers in a file of root hints, which need to be updated periodically by the local administrator from a reliable source to be kept up to date with the changes which occur over time.

Step 2: Query one of the root servers to find the server authoritative for the next level down (so in the case of our simple hostname, a root server would be asked for the address of a server with detailed knowledge of the example top level domain).

Step 3: Querying this second server for the address of a DNS server with detailed knowledge of the second-level domain (inadomain.example).

Step 4: Repeating the previous step to progress down the name, until the final step which would, rather than generating the address of the next DNS server, return the final address sought.

Figure 6.12shows the process for the real host www.thakur.org.

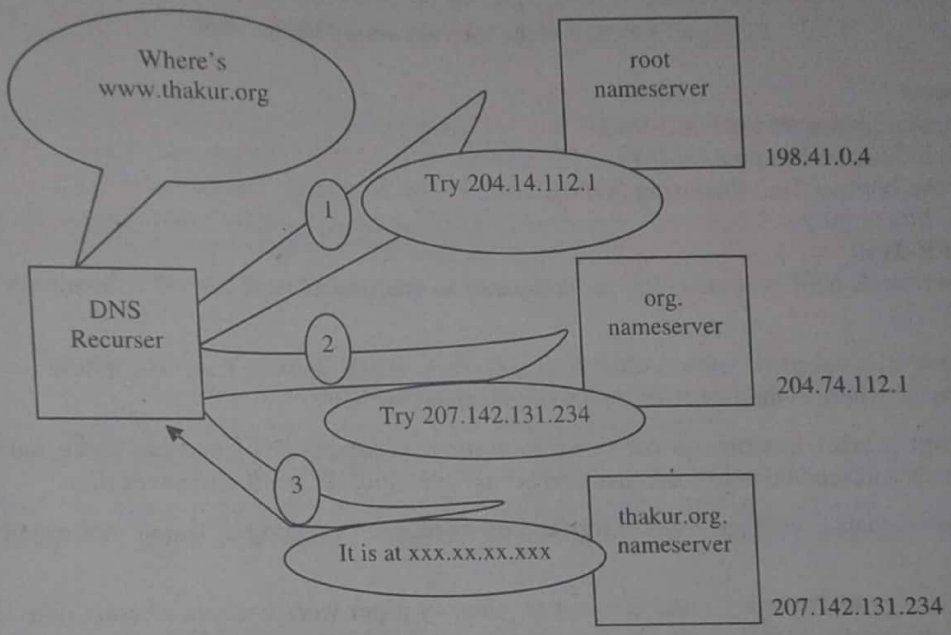


Figure 6.12 Process for the Real Host

The mechanism in this simple form has a difficulty: it places a huge operating burden on the root servers, with every search for an address starting by querying one of them.

Being as critical as they are to the overall function of the system, such heavy use would create an insurmountable bottleneck for trillions of queries placed every day. Caching is used to overcome this problem and in actual fact root nameservers deal with very little of the total traffic.

Ques 18) What is E-mail? What are the advantages and disadvantages of E-mail?

Or

What are the different e-mail protocols? List them.

Ans: Electronic Mail (E-Mail)

Electronic mail or e-mail, as it is popularly known, is a method of sending and receiving messages (mail) electronically over a computer network.

E-mail is a system allows a person or a group to electronically communicate to others through Internet.

A typed message is transmitted through the use of telephone line and high speed modem the message is send in the digital form which is a machine readable language and it is stored in the mail boxes of the receiver. Message can be retrieved by the concept of the receipt; users can edit, sort, classify and forward the message.

The concept of e-mail is not new. It was one of the first services to be used by the ARPANET community in the late 60s. Since then, the concept of e-mail became very popular. Today, all Internet Service Providers (ISP's) provide e-mail service at a reasonable cost.

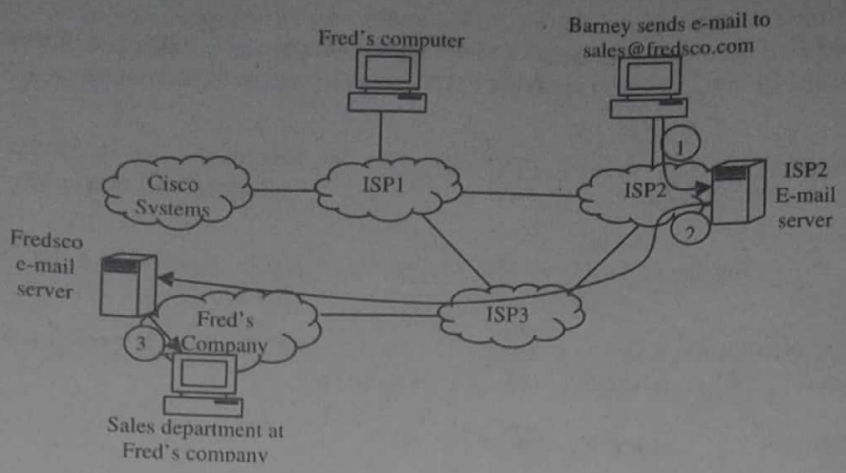


Figure 6.13 E-Mail in the Internet using Mail Servers

E-Mail Protocols

There are two main **protocols** used in E-Mails:

1) Simple Mail Transfer Protocol (SMTP)
2) Multipurpose Internet Mail Extension (MIME)

Advantages of E-Mail

1) **Cost Effective:** E-mail is least costly as compared to traditional methods of transmitting information like fax or courier.
2) **High Speed:** The speed of transmitting messages *via* e-mails is very fast. So, within seconds one can send the messages to anywhere in the world. It can also be received instantly.
3) **Time Saving:** It takes less time as compared to writing on papers. Even one can make multiple copies of message within seconds and send them to more than one person at a time. Hence, it also saves time.
4) **Easy to Use:** E-mail is very easy to use for sending or receiving messages. It does not require intense knowledge of computer.
5) **Reduces Wastage of Papers:** E-mail does not require any paper work because messages are written in soft copies. It also reduces the burden of maintenance.
6) **Message Storage Facility:** Message storing facility is also provided by e-mail for future reference.

Disadvantages of E-Mail

1) **Hardware Requirement:** Sending messages *via* e-mails require some hardware like computer and modem for Internet connection. Without Internet connection one cannot send mails.
2) **Lack of Expressions:** Matter typed over computer cannot express feelings. So, e-mail doesn't deliver sender's feeling and expressions to the recipient.
3) **Virus:** Sometimes e-mails may bring virus with them that can harm your computer system. Virus is a small program that may read your e-mail address book and transfer it to other person.
4) **Spam:** Spams are the unwanted or useless e-mails. It is very difficult task to separate the unwanted e-mails from the important ones.

Ques 19) What is SMTP? Also explain the working of SMTP.

Ans: Simple Mail Transfer Protocol (SMTP)

It is a set of communication guidelines that allow software to transmit email over the Internet. Most email software is designed to use SMTP for communication purposes when sending email and it only works for outgoing messages. When people set up their email programs, they will typically have to give the address of their Internet service provider's SMTP server for outgoing mail.

This protocol is used for the delivery of e-mail. When an E mail is to be sent, then the Mail Transfer Program contacts the remote machine and forms a TCP connection over which the mail is transferred. Once the connection is established, then Simple Mail Transfer Protocol (SMTP) identifies the sender itself, specifies the recipient of mail and then transfers the E mail message.

SMTP provides a set of codes that simplify the communication of e-mail messages between servers. It is a kind of shorthand that allows a server to break up different parts of a message into categories the other server can understand. Any email message has a sender, a recipient - or sometimes multiple recipients - a message body, and usually a title heading.

From the perspective of users, when they write an email message, they see the slick interface of their email software, but once that message goes out on the Internet, everything is turned into strings of text. This text is separated by code words or numbers that identify the purpose of each section. SMTP provides those codes, and email server software is designed to understand what they mean.

The other purpose of SMTP is to set up communication rules between servers. **For example,** servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. There are also ways to handle errors, including common things like incorrect email addresses. In a typical SMTP transaction, a server will identify itself, and announce the kind of operation it is trying to perform.

The other server will authorise the operation, and the message will be sent. If the recipient address is wrong, or if there is some other problem, the receiving server may reply with an error message of some kind.

Working of SMTP

i) **Composition of Mail:** A user sending an e-mail starts by composing an electronic mail message using an authenticated mail client (Mail User Agent – MUA). The message contains the body and the header. The body is the main part of the message while the header contains control information like the sender and recipient e-mail addresses. Headers also include descriptive information like the subject and message submission date/time stamp.

This is analogous to real mail, where the message body is like a letter and the header is like the envelope containing the recipient's address and a return address.

ii) **Submission of Mail:** The mail client then submits the completed e-mail to the configured SMTP server or mail server (Mail Submission Agent – MSA) using SMTP on TCP port 25 or 587, which acts as an electronic post-office. This is similar to how letters gets dropped off at the post-office for sorting and delivery.

iii) **Delivery of Mail:** E-mail addresses like john@email.com are sorted in a similar way. The "john" portion in the address is the username of the recipient and "email.com" is the domain name, similar to a postal address. If the domain name of the recipient's e-mail address is different from the sender, MSA will hand the mail over to the Mail Transfer Agent (MTA).

The role of MTA is to relay e-mails containing recipient e-mail addresses with different domain names – similar to how post-office transfer letters addressed to a different state/country. MTA also uses SMTP to receive e-mails relayed from other MTAs.

To relay the e-mail, the MTA must first locate the target domain. It does this by requesting for the Mail Exchanger record (MX record) from the Domain Name System (DNS). The MX record contains the name and Internet Protocol (IP) address of the recipient's domain. IP addresses are similar to postal codes. Once the record is located, MTA connects to the exchange server to relay the message.

iv) **Receipt and Processing of Mail:** Once the incoming message is accepted, the exchange server delivers it to the incoming mail server (Mail Delivery Agent MDA) which stores the e-mail where it waits for the user to retrieve it. This is equivalent to the real world example where the recipient's local post office delivers the mail into an individual's post office boxes.

v) **Access and Retrieval of Mail:** The stored e-mail can be retrieved by authenticated mail clients (MUAs). By using a login and password to access the MUA, MDA ensures individual users only have the right to access their own e-mails. Instead of SMTP, e-mail clients use either Internet Message Access Protocol (IMAP) or Post-Office Protocol (POP) to retrieve e-mails. POP is used for retrieving e-mails while IMAP manages and facilitate access to mail. Unlike SMTP, POP and IMAP are specifically designed to retrieve messages.

Ques 20) Discuss about the MIME?

Ans : Multipurpose Internet Mail Extension (MIME)

The MIME specification includes the following **elements:**

1) Five new message **header fields** are defined. These fields provide information about the body of the message.
2) A number of content formats are defined, thus standardising representations that support multimedia electronic mail.
3) Transfer encodings are defined that enable the conversion of any content for mat into a form that is protected from alteration by the mail system.

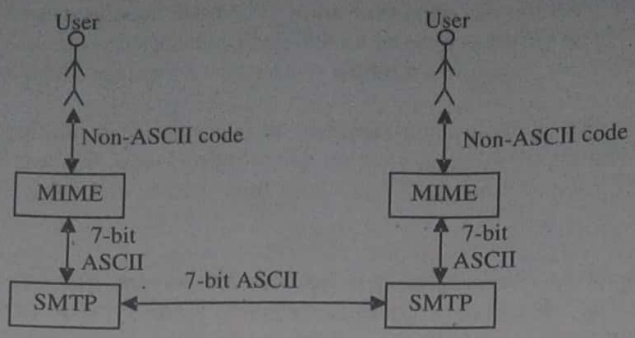


Figure 6.14: Working of MIME

Header Fields

1) **MIME-Version:** It identifies the MIME version. These simply tell the user agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses. Any message not containing a MIME-Version: header is assumed to be an English plaintext message, and is processed as such.

2) **Content-Description:** It is a human-readable string what is in the message. Header is an ASCII string telling what is in the message. This header is needed so the recipient will know whether it is worth decoding and reading the message.

3) **Content - ID:** It is a unique identifier. Header identifies the content. It uses the same format as the standard message-Id: header.

4) **MIME Content Types:** There are seven different major types of content and a total of 15 subtypes. In general, a content type declares the general type of data, and the subtype specifies a particular format for that type of data.

Type	Subtype	Description
Text	Plain	Unformatted text
	Richtext	Text including simple formatting commands
Image	GIF	Still picture in GIF format
	JPEG	Still picture in JPEG format
Audio	Basic	Audible sound
Video	MPEG	Movie in MPEG format
Application	Octet-stream	An un-interpreted byte sequence
	Postscript	A printable document in PostScript
Message	RFC822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

The application type is a catchall for formats that require external processing not covered by one of the other types. The message type allows one message to be fully encapsulated inside another. This scheme is useful for forwarding e-mail.

The final type is multipart, which allows a message to contain more than one part, with the beginning and end of each part being clearly delimited.

5) **Content – Transfer – Encoding:** Tells how the body is wrapped for transmission through a network that may object to most characters other than letters, numbers, and punctuation marks. Five schemes (plus an escape to new schemes) are provided. The simplest scheme is just ASCII text. The objective is to provide reliable delivery across the largest range of environments.

The Content-Transfer-Encoding field can actually take on six values, as listed in **table 6.3**. However, three of these values (7bit, 8bit and binary) indicate that no encoding has been done but provide some information about the nature of the data. For SMTP transfer, it is safe to use the 7bit form, The 8bit and binary forms binary forms may be usable in other mail transport contexts. Another Content-Transfer-Encoding value is x-token, which indicates that some other encoding scheme is used, for which a name is to be supplied.

This could be a vendor-specific or application-specific scheme. The two actual encoding schemes defined are quoted-printable and base64.

Two schemes are defined to provide a choice between a transfer technique that is essentially human readable and one that is safe for all types of data in a way that is reasonably compact.

Table 6.3: MIME Content – Transfer Encoding

7bit	The data are all represented by short lines of ASCII characters.
8bit	The lines are short, but there may be non-ASCII characters (octets with the high-order bit set).
binary	Not only may non-ASCII characters be present, but the lines are not necessarily short enough for SMTP transport.
quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters.
x-token	A named nonstandard encoding.

A compliant implementation must support the MIME – Version, Content – Type, and Content – Transfer – Encoding fields; the Content – ID and Content-Description fields are optional and may be ignored by the recipient implementation.

Ques 21) What is SNMP? What are the key elements of network management?

Ans: Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

Simple Network Management Protocol (SNMP) is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

A network management system is a collection of tools for network monitoring and control that is integrated. **Figure 6.15** shows the network management using SNMP. A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network management tasks resides in the host computers and communications processors (e.g., networks switches, routers).

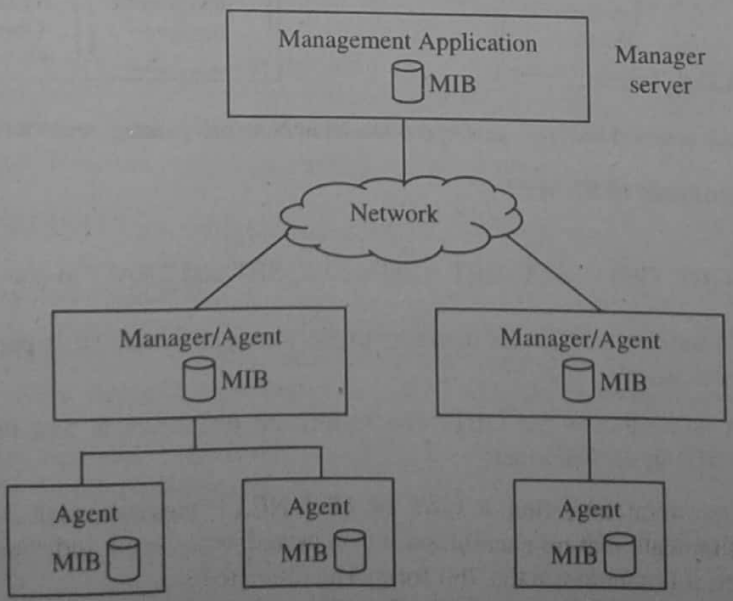


Figure 6.15: Network Management using SNMP

A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of each element and link known to the system. The active elements of the network provide regular feedback of status information to the network control center.

Elements of Network Management

The key elements of network management are:

1) **Management Station:** The management station provides the Human Machine Interface (HMI) to monitor and control the network. It contains the set of applications for data analysis and fault recovery. It provides a graphical user interface to manage the network through simple commands or mouse-clicks. It has the complete database of network management information.

2) **Agents:** This is the software residing in the bridges, routers, hosts, and such for remote management. This software will send the necessary data based on the commands from the management station.

3) **Management Information Base (MIB):** Data variables (objects) represent one aspect of a managed agent. The collection of objects is the MIB. **For example,** for a packet switch, the buffer size, the number of packets dropped, the delay, and so on can be the variables.

4) **Network Management Protocol:** This is SNMP (Simple Network Management Protocol) in TCP/IP networks and CMIP (Common Management Information Protocol) in ISO/OSI networks. SNMP runs on the UDP and not TCP. Because the network management information is not of very high priority, UDP is used instead of TCP.

Ques 22) What is the manager/agent model?

Ans: Manager/Agent Model

SNMP is based on the manager/agent model consisting of an SNMP manager, an SNMP agent, database of management information, managed SNMP devices and the network protocol. SNMP manager provides the interface between the human network manager and the management system. SNMP agent provides the interface between the manager and the physical device(s) being managed.

SNMP manager and agent use an SNMP Management Information Base (MIB) and a relatively small set of commands to exchange information. SNMP MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A long numeric tag or Object Identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

Figure 6.16 shows that SNMP is based on the Manager/Agent Model of Network Management Architecture.

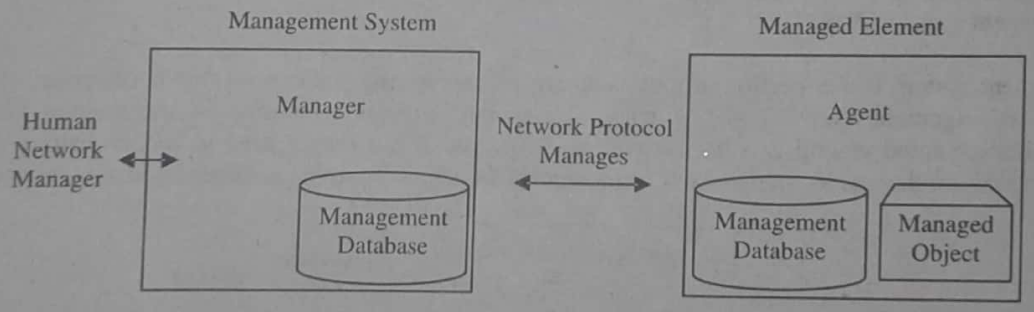


Figure 6.16: SNMP is based on Manager/Agent Model of Network Management Architecture

Ques 23) What are the basic commands of SNMP?

Ans: Basic Command of SNMP

SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET and TRAP) to communicate between SNMP manager and SNMP agent:

1) **GET:** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.

2) **GET NEXT:** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.

3) **GET-RESPONSE:** The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the SNMP manager with either the information requested or an error indication as to why the request cannot be processed.

4) **SET:** A SET message allows the SNMP manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. SNMP agent will then respond with a GET-RESPONSE message indicating the change has been made or an error indication as to why the change cannot be made.

5) **TRAP:** SNMP TRAP message allows the agent to spontaneously inform the SNMP manager of an "important" event.

Ques 24) What is Management Information Base (MIB)?

Ans: Management Information Base (MIB)
Each SNMP element manages specific objects with each object having specific characteristics. Each object/characteristic has a unique Object Identifier (OID) consisting of numbers separated by decimal points (i.e., 1.3.6.1.4.1.2682.1). These object identifiers naturally form a tree as shown in **figure 6.17**.

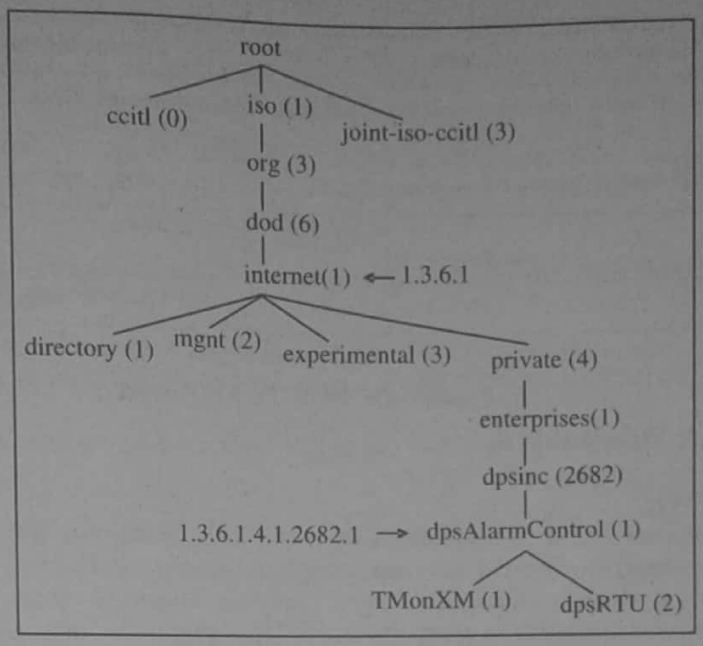


Figure 6.17: Object Identifiers Tree

The MIB associates each OID with a readable label (i.e., dpsRTUAState) and various other parameters related to the object. The MIB then serves as a data dictionary or code book that is used to assemble and interpret SNMP messages.

When an SNMP manager wants to know the value of an object/characteristic, such as the state of an alarm point, the system name or the element uptime, it will assemble a GET packet that includes the OID for each object/characteristic of interest.

The element receives the request and looks up each OID in its code book (MIB). If the OID found (the object is managed by the element), a response packet is assembled and sent with the current value of the object/characteristic included. If the OID is not found, a special error response is sent that identifies the unmanaged object.

When an element sends a TRAP packet, it can include OID and value information (bindings) to clarify the event. DPS remote units send a comprehensive set of bindings with each TRAP to maintain traditional telemetry event visibility. Well-designed SNMP managers can use the bindings to correlate and manage the events. SNMP managers will also generally display the readable labels to facilitate user understanding and decision-making

Ques 25) Discuss about the SNMP packet types and structure.

Ans: SNMP Packet Types and Structure
The Simple Network Management Protocol (SNMP) examines the communication between managers and agents. Basic serial telemetry protocols, like TBOS, are byte oriented with a single byte exchanged to communicate. Expanded serial telemetry protocols, like TABS, are packet oriented with packets of bytes exchanged to communicate.

The packets contain header, data and checksum bytes. SNMP is also packet oriented with the following SNMP v1 packets (Protocol Data Units or PDUs) used to communicate:
1) Get,
2) GetNext,
3) Set,
4) Trap.

The manager sends a Get or GetNext to read a variable or variables and the agent's response contains the requested information if managed. The manager sends a Set to change a variable or variables and the agent's response confirms the change if allowed. The agent sends a Trap when a specific event occurs.

The **figure 6.18** shows the packet formats. Each variable binding contains an identifier, a type and a value (if a Set or response). The agent checks each identifier against its MIB to determine whether the object is managed and changeable (if processing a Set). The manager uses its MIB to display the readable name of the variable and sometimes interpret its value.

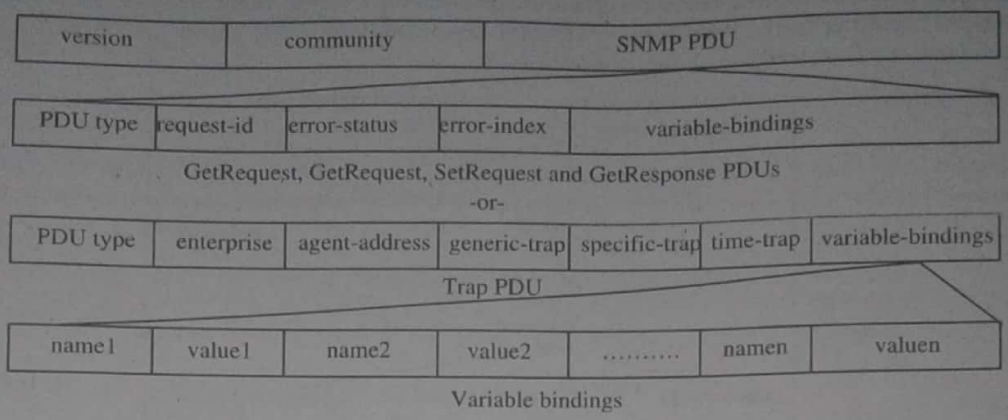


Figure 6.18: SNMP Packet Format

Ques 26) What is World Wide Web(WWW)?

Ans: World Wide Web(WWW)
WWW is the most popular internet tool. It is also known as **Web**. With the help of WWW, users can easily access and present the documents on the internet. These documents stored on the server. In other words, web is a collection of interlinked hypertext documents which are accessed through internet. Hypertext documents are also known as 'Web Pages'. In a set of web pages (websites), the first one is called **Home Page**. The information is available on WWW via **HTTP** (Hypertext Transfer Protocol).

A system of 'interlinked hypertext documents' which can be accessed via the internet is referred to as the 'web'. TCP/IP is the fundamental transport mechanism used in the World Wide Web. Various companies set up websites which are collection of web pages. These pages are digitally stored on the 'Web server'. The web is thus a collection of pages which are interlinked on a global scale. A 'web browser' helps in viewing the web pages. It uses the HTTP protocol (language spoken over the internet) for the trar.smission of data. Web services help in exchange of business ideas and usage of web for information sharing.

Web uses browsers like Internet Explorer or Google Chrome for accessing the 'web pages' which are text files, created using HTML code. Web pages may also contain JavaScript code and other commands. Each web page may be a union of text, pictures, audio clips, animations and other data which can be electronically presented. Web pages use **hyperlinks** for navigation on the web (internet).

On the request of a client a web page (stored on the disk of a 'web server') is sent to the client. Web pages contain tags (written in a codified form). These tags are used to decide how the web pages are visible on the client's monitor. To open a website a web address is necessary which is known as **Uniform Resource Locator (URL)**. The World Wide Web is non-linear that means there is no bottom and a user needs not to follow a hierarchical route to information resources.

Therefore:
1) Clients may jump from one resource (link) to another.
2) Clients may directly access the resources if they know the webpage address or URL.
3) Clients can also access specific parts of a document.

Web handles the graphics and also provides flexibility in the organisation, presentation and description of the information resources.

Ques 27) What are the main features of WWW?

Ans: Features of WWW
The important features of WWW are:
1) **Hyperlinked:** A web page comprises of text, graphic objects, etc. which are also associated with other web pages. This type of association is known as **Hyperlink**. These can be hypertext or hypermedia. A hypertext can be defined as the coloured or underlined text. When user clicks on the hypertext he/she will reach a specific file, specific location in a file, or an HTML page on WWW.

2) **Graphical:** The interactive, graphic and multimedia part of the internet is the web. It comprises of databases, text, pictures, sounds, and digital movies.

3) **Easier Navigation:** Web browsers (i.e., Internet Explorer, Chrome, etc.) help the user to navigate on web by using the **Back, Forward, and History** features (available in the button format). It is easy for the user to navigate around a site as web pages contain hypertext as well as hypermedia links.

4) **Cross-Platform:** The internet uses open interconnection of computer systems which support multi-vendor environment. This helps in connection of system to devices and programs made by different manufacturers.

5) **Distributed:** Web comprises of the millions of websites where information is spread globally on the many 'web servers'.

6) **Dynamic:** Information can be accessed dynamically on web by clicking on the appropriate hyperlink. Websites never have the arrangement of data and information in the linear fashion so one can access (by clicking on a link) any page randomly.

7) **Interactive:** Web pages also have the interactive forms that one can fill and submit. With the help of this interactive form one can easily communicate with the website or web page publishers.

8) **Supports Various Protocols:** Web uses HTTP for communication and information sharing but it also supports various other protocols such as FTP, Telnet, Gopher, etc., as they too are part of internet.

Ques 28) Draw the WWW architecture? Also discuss about the different components of WWW?

Ans: WWW Architecture

The general architecture of the World Wide Web is 'two tiered'. This architecture has a 'web client' which displays the information content and a 'web server' which provides information to the client (when requested).

For e-commerce applications this architecture works as basis. It develops software where functions are spread over the application servers (where applications exist), data servers (where data are stored) and collection of networked PCs (which are used by the information users).

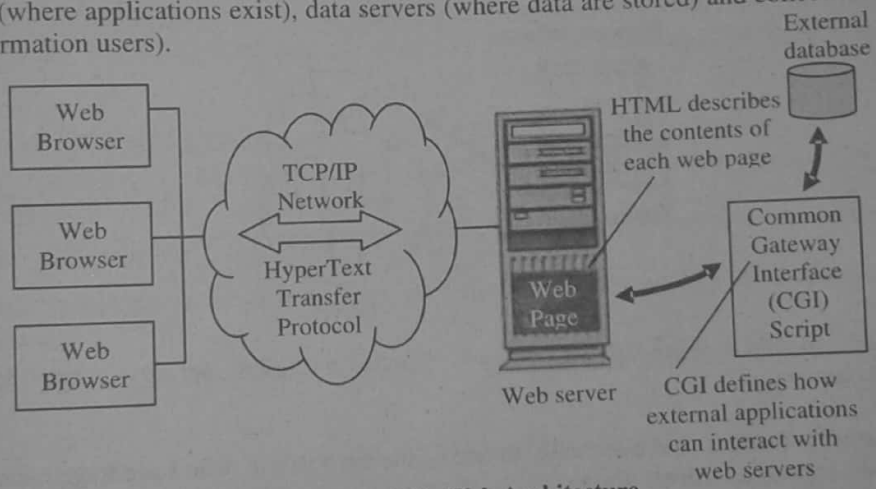


Figure 6.19: Web Architecture

Figure 6.19 depicts the web architecture. The various components of web architecture are:

1) Web Clients,
2) Web Servers,
3) HTTP Protocol, and
4) Applications.

These components cooperate to ensure a smooth change from today's computing resources to those of tomorrow. This is achieved by incorporation of information access and exchange within a specific business application.

Components of World Wide Web

The components of the web are as follows:

1) **Web Clients:** Web clients are also referred to as browsers which provide a graphical user interface for content display. These may run on IBM-compatible PCs, Apple Macintosh computers, UNIX platforms and other platforms which provide a number of facilities. Following are the few most popular browsers:
   i) Microsoft's Internet Explorer,
   ii) Firefox Mozilla, and
   iii) Google's Chrome.

2) **Web Servers:** Web servers are group of both software and hardware that act as information storehouses. These programs can be executed over IBM PCs, Apple Macintosh computers, UNIX platforms, etc. The most popular web clients are Microsoft's Internet Information Server and Netscape's Communications Server.

3) **Hypertext Markup Language (HTML):** This language is used for creating the documents and webpages. It uses a variety of tags and attributes which define the structure and layout of the web document.

4) **Uniform Resource Locater (URL):** The Uniform Resource Locator is a unique address assigned to a specific website or web page. This is entered in the address bar of the browser to visit a particular site or page.

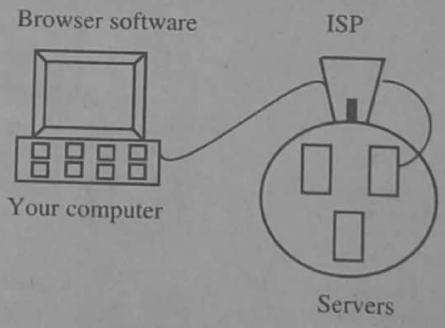
5) **Hypertext Transfer Language (HTTP):** HTTP is the protocol which guides the working of the web. This protocol decides how a message is formatted and transmitted over the internet. It also takes the decision that what will be the action of servers and browsers in response to the different commands. **For example,** when an URL is entered in the address bar, a HTTP command goes to the server that directs the server to fetch the requested web page and transmit it to the client. Thus, messages are sent and received on the web via HTTP.

6) **CGI (Common Gateway Interface):** CGI is a standard for web server to transfer the web user's request to an application program and also transferring the received data back to the user. **For example,** when the user requests an URL, the server will immediately display the requested page. But when a user fills out a form and submits it on a web page, it is processed by an application program. The server sends the information to a small application program which processes the information and sends back a confirmation. This process of sending and receiving message to and from between the server and the application is referred to as Common Gateway Interface (CGI) which is a part of HTTP.

Ques 29) Explain the working of WWW.

Ans: Working of World Wide Web (WWW)

On the web, navigate through pages of information based on what interests you at that particular moment. This is commonly known as browsing or surfing the net. To access web we need software such as Internet Explorer, Netscape Navigator known as web browser. Web pages are written in computer language called **HTML**.



System has a unique number assigned to it (and IP address), is connected to the Internet service provider possibly through **dial-in modem** or by direct connection.

ISP in turn is connected to other providers, and eventually to one of the big carriers, who have huge networks that use **fiber optic cables** running at 45 mb/second as **shown above**.

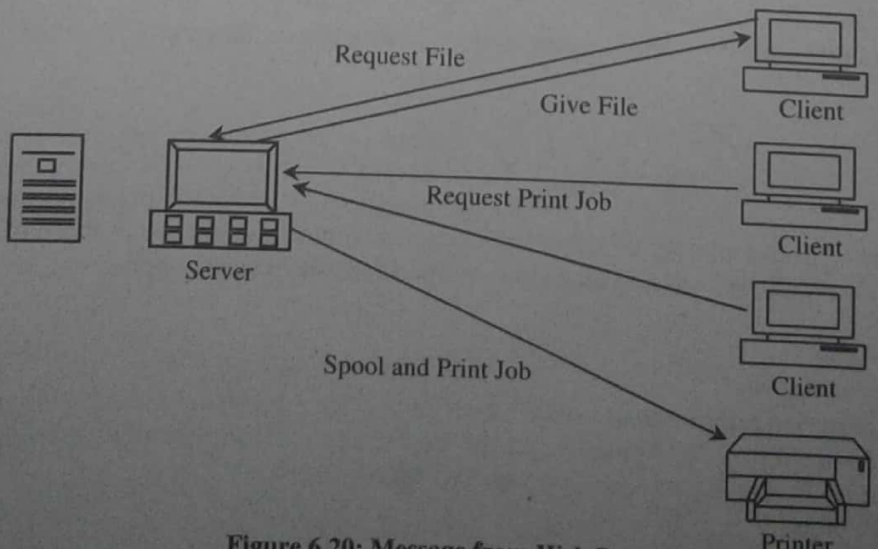


Figure 6.20: Message from Web Browser

Ques 30) What are the advantages and disadvantages of WWW?

Ans: Advantages of WWW

Web has many advantages; some of them are as follows:

1) **Establish a Presence:** More than seven million people access the web every day with more numbers being added daily. Businesses want to tap this large community of people for expanding their business. Thus, most companies develop a website, which could be an online store, open 24 hours in a day thereby increasing their sales and profits.

2) **Networking:** It helps in communication between potential clients and organisations.

3) **Provide Business Information:** Like traditional print advertising, websites also contain information about business hours, location, e-mail, etc. for public viewing with instant communication of any changes in the previous details. **For example,** customers can check availability of seats at restaurants and check their menu or what is the special dish of the day and so on, so that they can make an informed decision. Details of a company or organisation are just a few clicks away.

4) **Service your Customers:** Customers can have access to certain business information and services, which are not available in any other place and media. In case of online retailing or e-tailing, customers can purchase the goods and services from any location of the world.

5) **Conduct Business:** For an online portal to be successful commercially, it needs to do certain things to expand business. Like, website provides tools to locate exact products that are required to the customer as well as provide forms that need to be submitted by the customers to buy the product or service online. This can be achieved automatically without human intervention 24 hours a day.

6) **Provide Files to Download:** A company's website can offer all brochures, advertisements and even demonstration video of product or service in downloadable form. This is done with an intention of providing an interactive and effective introduction of the company's products and services to the potential clients.

7) **Remote Employee/Office Access:** Employees who are travelling needs access to the up-to-date information to complete the work. Important and sensitive information are password protected for the employees and they can access this information by logging into 'office' any time from any place of the world by paying a small cost.

Disadvantages of WWW

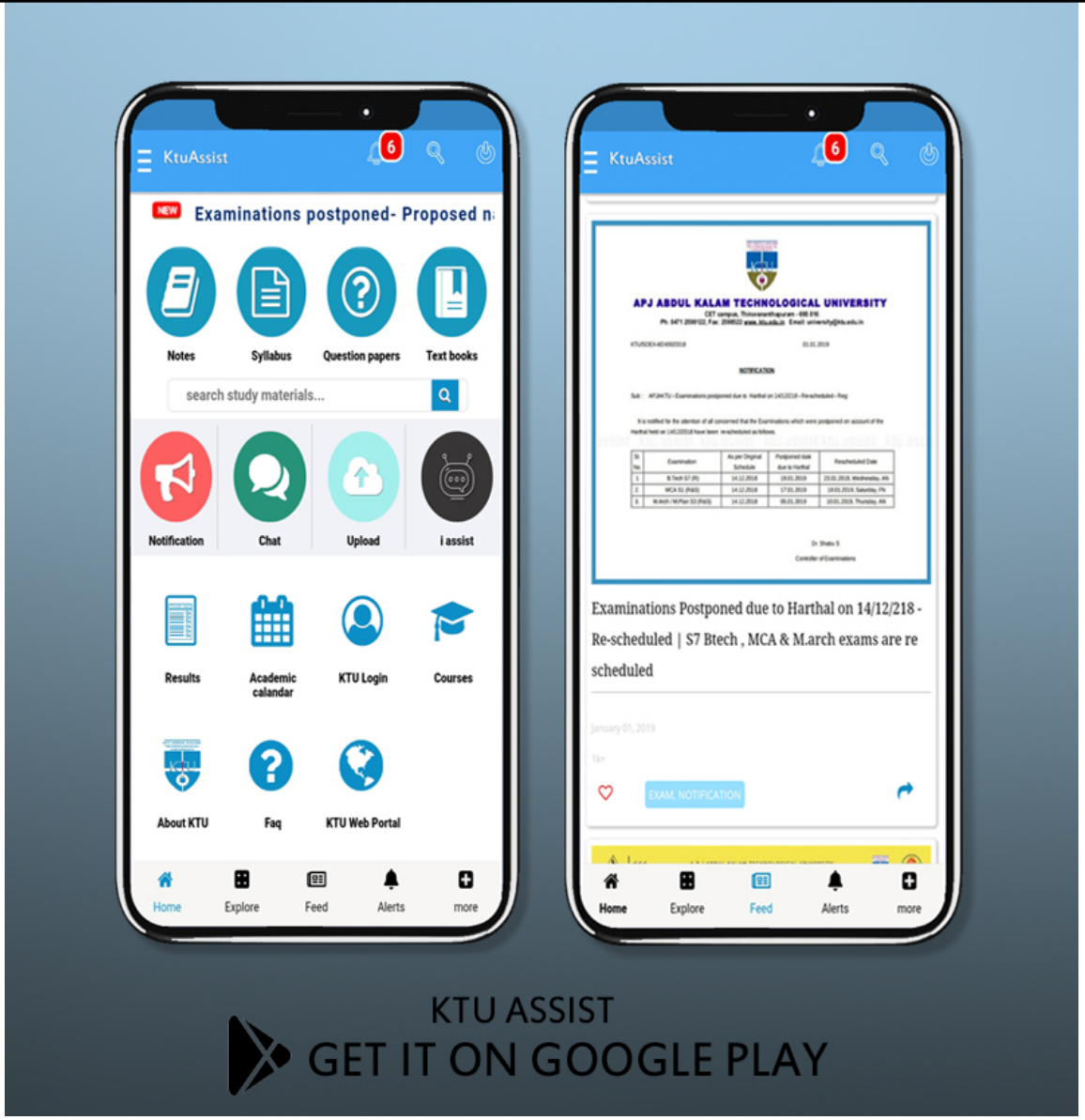
Certain disadvantages of web are as follows:

1) **Time Consuming:** It is time consuming, as a person may spend all his/her time on the internet instead of interacting with people face to face. This may isolate a person.

2) **Unreliable:** It may cause unreliable information sharing.

3) **Security Problem:** It might be a threat to national security. Maximum-security problem occur on the internet because of the human mistakes.

4) **Fraud:** It gives rise to the fraudulent activities as the web provides anonymity and ease of promotion without borders.



END

facebook.com/ktuassist

instagram.com/ktu_assist