Program : **B.E**

Subject Name: **Advance Computer Networks**

Subject Code: **CS-8004**

Semester: **8th**

Advance Computer Networks

Subject Notes: UNIT-II

# TCP/IP Reference Model

Basic Concepts: TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.

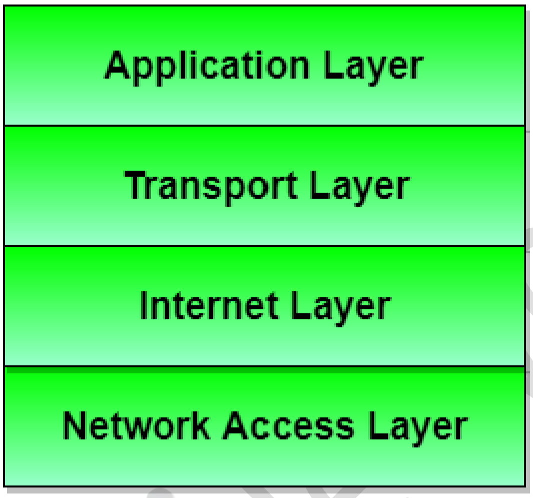


Fig. 2.1 TCP/IP Reference Model

#Protocols and networks in the TCP/IP model:

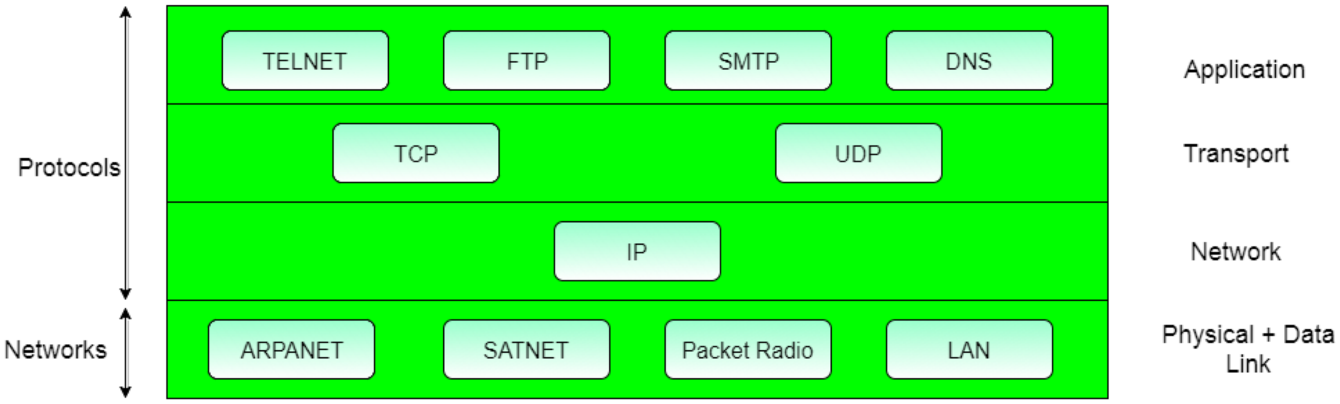


Fig. 2.2 Protocols and networks in the TCP/IP model

#Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

#Different Layers of TCP/IP Reference Model

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

#Connection Oriented & Connectionless Services

• Connection-oriented

There is a sequence of operation to be followed by the users of connection-oriented service. They are:

1. Connection is established
2. Information is sent
3. Connection is released

In connection-oriented service we must establish a connection before starting the communication. When connection is established we send the message or the information. Then we release the connection. Connection oriented service is more reliable than connectionless service. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

• Connectionless

It is similar to postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

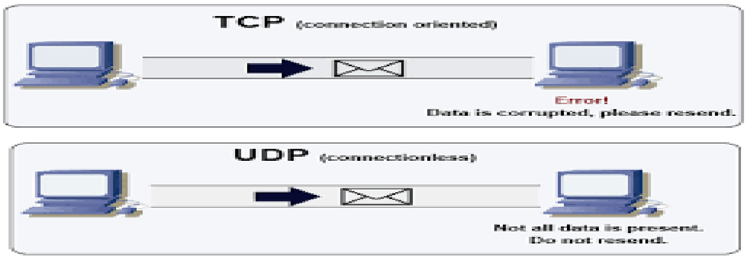


Fig. 2.3 Connection Oriented & Connectionless Services

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - TCP(Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   - UDP(User-Datagram Protocol): It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers**.**

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

# Principles of TCP/IP Reference Model

Centralized computer systems - the concept of 'computer center' where a large computer serves the entire organization has been replaced by 'computer network' - a large number of independent computers that are linked together in a network that can exchange information. The network allowed the following:

- Sharing Of Resources - Data, Programs, Equipment Available to everyone on The Network Regardless of Physical Distance,
- Reliability - Data Stored On Multiple Machines Because of Possible Failure,
- Savings - Instead Of Fast But Expensive Large Computers Use Multiple Pcs And Ensures Scalability: Client-Server Model,
- Connection - Link Between Physically Separated Employees,
- Remote Access To Information - Finances, Shopping, Online Newspapers, Www,
- Communication - Email, Discussion Groups, Video Conference,
- Entertainment - Video On Demand, Interactive Video And Television, Games.

. The terminology used to comprehend its functionality is based on the following basic concepts:

- Host - Computer in the local network (application aspect).
- Sub network (subnet) - Transmits messages from one host of LAN to host a second LAN (communication aspect), has two components:
  - Transmission channel (transmission lines, channel) - Bits transmitted from computer to computer.
  - Router - Specialized computer that connect the transmission channels and decide at which the output channel to send data that arrives from the door
- Sub network makes the core of communication between themselves and this is a point-to-point (store-and-forward, packet-switched) communication between routers that are not directly connected by a cable, and is done so that packets sent from router to router. Router save the package and send it on when the output line works.
- Topology connecting routers is usually irregular.

#Address Handling Internet Protocol:

The Internet's basic protocol called IP for Internet Protocol. The protocol is assigned to interconnect networks do not have the same frame-level protocols or package level. There are two generations of IP packets, called IPv4 (IP version 4) and IPv6 (IP version 6).

• Internet Protocol (IP) of network layer contains addressing information and some control information that enables the packets to be routed.

• **IP has two primary responsibilities:**

1. Providing connectionless, best effort delivery of datagrams through a internetwork. The term best effort delivery means that IP does not provides any error control or flow control. The term connectionless means that each datagram is handled independently, and each datagram can follow different route to the destination. This implies that datagram sent by the same source to the same destination could arrive out of order.
2. Providing fragmentation and reassembly of datagrams to support data links with different maximum transmission unit (MTU) sizes.

#IP packet format

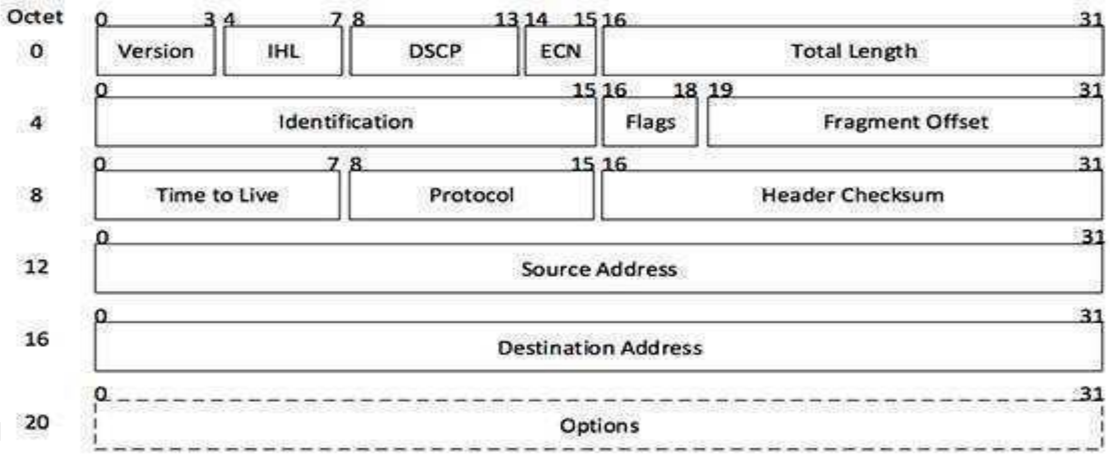
• Packets in the network layer are called datagram.

A datagram is a variable length packet consisting of two parts: header and data.

• The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

• The various fields in IP header are:

1. Version: It is a 4-bit field that specifies the version of IP currently being used. Two different versions of protocols are IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).
2. IP Header Length (IHL): This 4-bit field indicates the datagram header length in 32 bit word. The header length i8 not constant in IP. It may vary from 20 to 60 bytes. When there are no options, the header length is 20 bytes, and the value of this field is 5. When the option field is at its maximum size, the value of this field is 15.



[Image: IP Header]

Fig. 2.4 IP packet Format

3. Services: This 8 hit field was previously called services type but is now called differentiated services.

The various bits in service type are:

• A 3-bit precedence field that defines the priority of datagram in issues such as congestion. This 3-bit subfield ranges from 0 (000 in binary) to 7 (111 in binary).

• After 3-bit precedence there are four flag bits. These bits can be either 0 or 1 and only one of the bits can have value of 1 in each datagram.

- **The various flag bits are:**

1. D : Minimize delay

2. T : Maximize throughout
3. R : Maximize reliability
4. C : Minimize Cost

The various bits in differentiated services are: The first 6 bits defined a code point and last two bits are not used. If the 3 rightmost bits are 0s, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation.

4. Total length: This 16 bit field specifies the total length of entire IP datagram including data and header in bytes. As there are 16 bits, the total length of IP datagram is limited to 65,535 (216 - 1) bytes.

5. Identification: This 16 bit field is used in fragmentation. A datagram when passing through different networks may be divided into fragments to match the network frame size. Therefore, this field contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.

6. Flags: Consists' of a 3 bit field of which the two low order bit DF, MF control fragmentation. DF stands for Don't Fragment. DF specifies whether the packet can be fragmented MF stands for more fragments. MF specifies whether the packet is the last fragment in a series of fragmented packets. The third or high order but is not used.

7. Fragment Offset: This 13 bit field indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

8. Time to Live: It is 8 bit field that maintain a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps the packet from looping endlessly.

9. Protocol: This 8 bit field indicates which upper layer protocol receives incoming packets after IP processing is complete.

10. Header Checksum: This 16 bit field contains a checksum that covers only the header and not the data.

11. Source IP address: These 32-bit field contains the IP address of source machine.

12. Destination IP address: This 32-bit field contains the IP address of destination machine.

13. Options: This field allows IP to support various options such as security, routing, timing management and alignment.

14. Data: It contains upper layer information.

#Protocol Layers

The communication between the nodes in a packet data network must be precisely defined to ensure correct interpretation of the packets by the receiving intermediate and the end systems. The packets exchanged between nodes are defined by a protocol - or communications language. There are many functions which may be needed to be performed by a protocol. These range from the specification of connectors, addresses of the communications nodes, identification of interfaces, options, flow control, reliability, error reporting, synchronization, etc.

The protocols are usually structured together to form a layered design (also known as a "protocol stack"). All major telecommunication network architectures currently used or being developed use layered protocol architectures. There is a distinction between the functions of the lower (network) layers, which are primarily designed to provide a connection or path between users to hide details of underlying communications facilities, and the upper (or higher) layers, which ensure data exchanged are in correct and understandable form. The upper layers are sometimes known as "middleware" because they provide software in the computer which converts data between what the applications programs expect, and what the network can transport. The transport layer provides the connection between the upper (applications-oriented) layers and the lower (or network-oriented) layers.

The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run distributed applications.

TELNET

- TELNET is a standard protocol. Its status is recommended.
- It is described in RFC 854 - TELNET Protocol Specifications and RFC 855 - TELNET Option Specifications.
- Telnet was the first application demonstrated on the four-IMP (Interface Message Processor) network installed by December 1969. The final edition took 14 more years to develop, culminating in Internet Standard #8 in 1983, three years after the final TCP specification was ratified.
- Telnet even predates internetworking and the modern IP packet and TCP transport layers.
- The TELNET protocol provides a standardized interface, through which a program on one host (the TELNET client) may access the resources of another host (the TELNET server) as though the client were a local terminal connected to the server.
- For example, a user on a workstation on a LAN may connect to a host attached to the LAN as though the workstation were a terminal attached directly to the host. Of course, TELNET may be used across WANs as well as LANs.
- Most TELNET implementations do not provide you with graphics capabilities.
- TELNET is a general protocol, meant to support logging in from almost any type of terminal to almost any type of computer.
- It allows a user at one site to establish a TCP connection to a login server or terminal server at another site.
- A TELNET server generally listens on TCP Port 23.

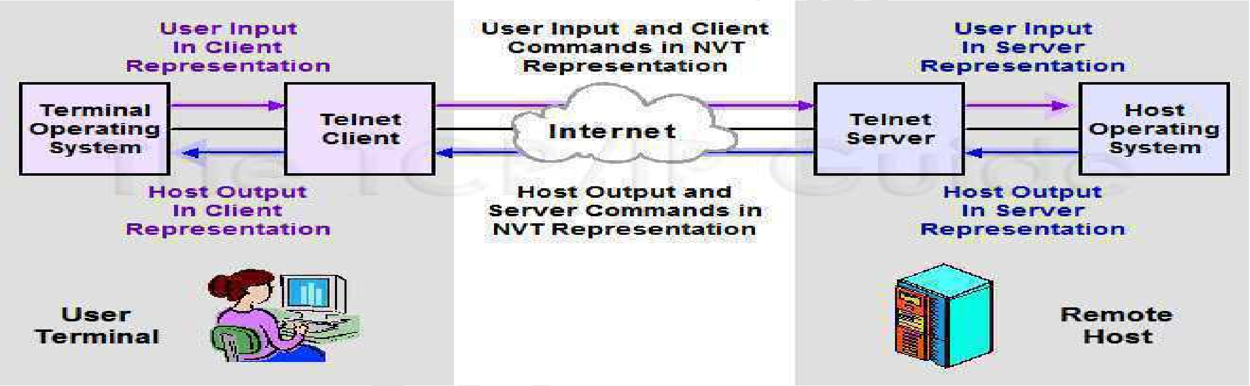


Fig. 2.5 TELNET Working

TELNET Operation

- The TELNET protocol is based on three ideas:
  - The Network Virtual Terminal (NVT) concept. An NVT is an imaginary device having a basic structure common to a wide range of real terminals. Each host maps its own terminal characteristics to those of an NVT, and assumes that every other host will do the same.
  - A symmetric view of terminals and processes .
  - Negotiation of terminal options. The principle of negotiated options is used by the TELNET protocol, because many hosts wish to provide additional services, beyond those available with the NVT. Various options may be negotiated. Server and client use a set of conventions to establish the operational characteristics of their TELNET connection via the ``DO, DON'T, WILL, WON'T'' mechanism discussed later in this document.
- The two hosts begin by verifying their mutual understanding. Once this initial negotiation is complete, they are capable of working on the minimum level implemented by the NVT.
- After this minimum understanding is achieved, they can negotiate additional options to extend the capabilities of the NVT to reflect more accurately the capabilities of the real hardware in use.

- Because of the symmetric model used by TELNET, both the host and the client may propose additional options to be used.
- The set of options is not part of the TELNET protocol, so that new terminal features can be incorporated without changing the TELNET protocol (mouse?).
- All TELNET commands and data flow through the same TCP connection.
- Commands start with a special character called the Interpret as Command escape character (IAC).
- The IAC code is 255.
- If a 255 is sent as data - it must be followed by another 255
- Each receiver must look at each byte that arrives and look for IAC. If IAC is found and the next byte is IAC - a single byte is presented to the application/terminal.
- If IAC is followed by any other code - the TELNET layer interprets this as a command.

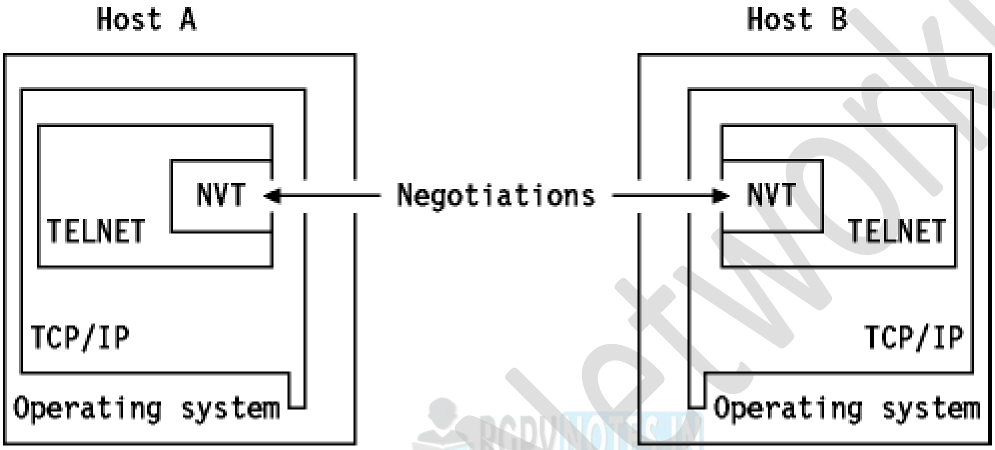


Fig. 2.6 TELNET Operations

#Rlogin (remote login)

Rlogin (remote login) is a UNIX command that allows an authorized user to login to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Once logged in to the host, the user can do anything that the host has given permission for, such as read, edit, or delete files.

Rlogin is similar to the better known Telnetcommand. Rlogin is considered useful for simple logins that don't require a lot of control over the client/host interaction, but is thought to be less useful than Telnet where a lot of customization is desired, for multiple sessions, for connections between very distant terminals or to terminals that are not running UNIX, for that matter, since rlogin can only connect to UNIX hosts. A benefit of rlogin is the ability to use a file called .rhosts that resides on the host machine and maintains a list of terminals allowed to login without a password.

A secure version of rlogin (slogin) was combined with two other UNIX utility, ssh and scp, in the Secure Shell suite, an interface and protocol created to replace the earlier utilities.

#Types of remote access

- Broadband provides remote users with high-speed connection options to business networks and to the internet. There are several types of broadband, including the following:
- Cable broadband shares bandwidth across many users and, as a result, upstream data rates can be slow during high-usage hours in areas with many subscribers.
- DSL (Digital Subscriber Line) broadband provides high-speed networking over a telephone network using broadband modem tech. However, DSL only works over a limited physical distance and may not be available in some areas if the local telephone infrastructure doesn't support DSL technology.
- Cellular internet services can be accessed by mobile devices via a wireless connection from any location where a cellular network is available.

- Satellite internet services use telecommunications satellites to provide users with internet access in areas where land-based internet access isn't available, as well as for temporary mobile installations.
- Fiber optics broadband technology enables users to transfer large amounts of data quickly and seamlessly.

#Remote access protocols

Common remote access and VPN protocols include the following:

- Point-to-Point Protocol (PPP) enables hosts to set up a direct connection between two endpoints.
- IPsec -- Internet Protocol Security -- is a set of security protocols used to enable authentication and encryption services to secure the transfer of IP packets over the internet.
- Point-to-Point Tunneling (PPTP) is one of the oldest protocols for implementing virtual private networks. However, over the years, it has proven to be vulnerable to many types of attack. Although PPTP is not very secure, it persists in some cases
- Layer Two Tunneling Protocol (L2TP) is a VPN protocol that does not offer encryption or cryptographic authentication for the traffic that passes through the connection. As a result, it is usually paired with IPsec, which provides those services.
- Remote Authentication Dial-In User Service (RADIUS) is a protocol developed in 1991 and published as an Internet Standard track specification in 2000 to enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that was originally common to Unix networks that enables a remote access server to forward a user's password to an authentication server to determine whether access to a given system should be allowed. TACACS+ is a separate protocol designed to handle authentication and authorization, and to account for administrator access to network devices, such as routers and switches.

#TFTP - Trivial File Transfer Protocol (TFTP)

Trivial file transfer protocol (TFTP) is suited for those applications that do not require complex procedures of FTP and do not have enough resources (RAM, ROM) for this purpose.

• Typical applications of TFTP include loading the image on diskless machine and upgrading the operating system in network devices such as routers.

The main features TFTP are:

1. TFTP is based on client/server principle.
2. It uses Well-known UDP port number 69 for TFTP server.
3. TFTP 1S unsecured protocol.
4. TFTP does not support authentication.

5 Every TFTP data unit has a sequence number.

6. Each data unit is individually acknowledged. After receiving the acknowledgement the next data unit is sent.
7. Error recovery is by retransmission after timeout.

#TFTP message formats

There are four types of TFTP messages. The first two octets indicate the type of message. Mode field defines the type of data (ASCII, binary, Mail). The filename and mode fields are delimited using an all zeroes octet.

1. Read request (Type 1). This is used by the client to get a copy of a file from the server.
2. Write request (Type 2). This command is used by the client to write a file into the server.
3. Data (Type 3) this command contains block of data (portion of the file being copied). This message contains the data block of fixed size of 512 octets. The session is terminated if a data message arrives with data octet less than 512 octets.
4. Acknowledgement (Type 4). The last data message can have data block with EOF having size less than 512 octets. This is used by the client and the server to acknowledge the received data units.

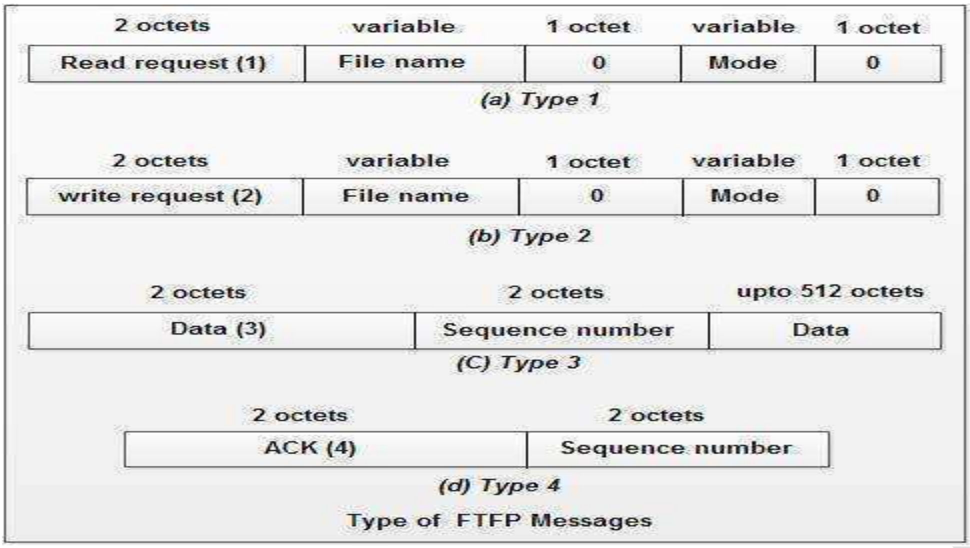


Fig. 2.7 Type of TFTP Messages

#TFTP Operation

- The client sends a read or write request at the server's UDP Port 69
- The server accepts the request by sending data message in case of read request.
- The server accepts the request by sending acknowledgement in case of write request.
- In either case, the server selects a UDP port to be used for further dialogue and sends its first response to the client through the selected UPD port.
- Each data message has fixed size of data block (512 octets) and IS individually acknowledged.
- The last data block containing EDF or a data block containing less than 512 octets terminates the session.
- Error recovery is done using retransmission after timeout.
- If TFTP message is lost and if there is no expected response, the message is repeated by the sender after time out.
- If the next data message is not received after acknowledgement, the last acknowledgement is repeated after timeout.

#Network File System (NFS)

The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were on the user's own computer. The NFS protocol is one of several distributed file system standards for network-attached storage (NAS).NFS allows the user or system administrator to mount (designate as accessible) all or a portion of a file system on a server. The portion of the file system that is mounted can be accessed by clients with whatever privileges are assigned to each file (read-only or read-write). NFS uses Remote Procedure Calls (RPC) to route requests between clients and servers.

NFS was originally developed by Sun Microsystems in the 1980's and is now managed by the Internet Engineering Task Force (IETF). NFSv4.1 (RFC-5661) was ratified in January 2010 to improve scalability by adding support for parallel access across distributed servers. Network File Sytem versions 2 and 3 allows the User Datagram Protocol (UDP) running over an IP network to provide statelessnetwork connections between clients and server, but NFSv4 requires use of the Transmission Control Protocol (TCP).

#Post Office Protocol version 3 (POP3)

It is a simple protocol used for opening the remote e-mail boxes. This protocol is defined in RFC 1225. Post Office Protocol version 3 (POP3) is a message access protocol that enables the client to fetch an e-mail from the remote mail server. SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time; otherwise TCP connection cannot be established. The server receives the mail on behalf of its clients. A POP3 server stores messages for each user until the user connects to download and read them using a POP3 client such as Microsoft Outlook 98, Microsoft Outlook Express, or Microsoft

Mail and News. To retrieve a message from a POP3 server, a POPS client establishes a Transmission Control Protocol (TCP) session using TCP port 110, identifies itself to the server, and then issues a series of POP3 commands:

1. stat: It asks the server for the number of messages waiting to be retrieved.
2. list: It determines the size of each message to be retrieved.
3. retr: It retrieves individual messages d. Quit: Ends the POP3 session.

Mail access by POP3

• The client POP3 software is installed on the receiver's computer the server POP3 software is installed on the mail server.

• POP3 is described in RFC 1939 and it uses well-known TCP port 110.

• The communication procedure is similar to SMTP and uses ASCII characters.

• POP3 begins when user starts the mail reader.

• The mail reader calls up the ISP (or mail server) and establishes a TCP connection with the message transfer agent at port 110.

• Once the connection has been established, the PO?3 protocol goes through three states in sequence

1. Authorization
2. Transactions
3. Update

• The Authorization state deals with user log in. The client sends its user name and password.

• The transaction state deals with the user collecting the e-mails and marking them for deletion from the mailbox.

• The update state causes the e-mails to be deleted.

• Once the user has logged in, the client can send the LIST command to list the contents of its mailbox. In this case the server displays one message per line along with its length. This list ends with a period.

• The client can retrieve messages using RETR command and can also mark them for deletion with DELE.

• When all the messages have been retrieved, the client gives QUIT command to end the transaction state and enter the update state.

• When the server has deleted all the messages, it sends a reply and breaks the TCP connection.

• Although POP3 is used to download messages from the server, the SMTP client is still needed on the desktop computers to forward messages from workstation user to its SMTP mail server.

POP3 protocol works on two ports:

Port 110 - this is the default POP3 non-encrypted port

Port 995 - this is the port you need to use if you want to connect using POP3 securely

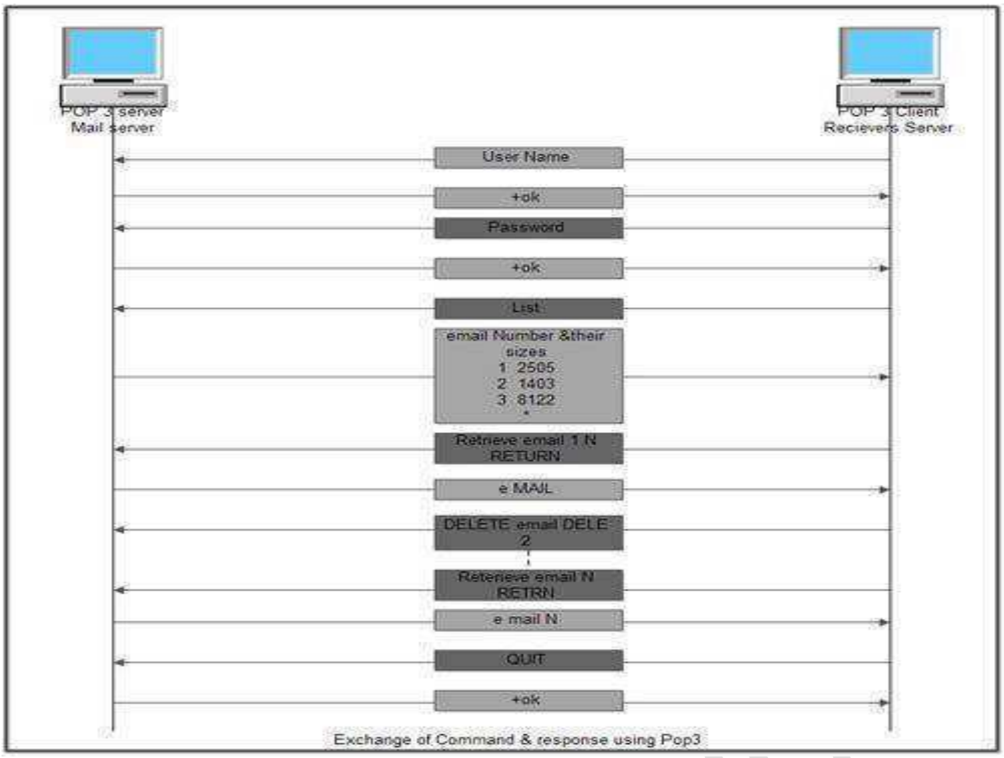


Fig. 2.8 Exchange of Command and Response using POP3

#Internet Message Access Protocol (IMAP)

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

Port 143 - this is the default IMAP non-encrypted port

Port 993 - this is the port you need to use if you want to connect using IMAP securely

#Multipurpose Internet Mail Extension (MIME)

Multipurpose Internet Mail Extension (MIME) is a standard which was proposed by Bell Communications in 1991 in order to expand limited capabilities of email.MIME is a kind of add on or a supplementary protocol which allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

Purpose and Functionality of MIME –

Growing demand for Email Message as people also want to express in terms of Multimedia. So, MIME another email application is introduced as it is not restricted to textual data.MIME transforms non-ASCII data at sender side to NVT 7-bit data and delivers it to the client SMTP. The message at receiver side is transferred back to the original data. As well as we can send video and audio data using MIME as it transfers them also in 7-bit ASCII data.

Features of MIME –

- It is able to send multiple attachments with a single message.
- Unlimited message length.
- Binary attachments (executables, images, audio, or video files) which may be divided if needed.
- MIME provided support for varying content types and multi-part messages.
- MIMEHeader:
  It is added to the original e-mail header section to define transformation. There are five headers which we add to the original header:

- MIME Version – Defines version of MIME protocol. It must have the parameter Value 1.0, which indicates that message is formatted using MIME.
- Content Type – Type of data used in the body of message. They are of different types like text data (plain, HTML), audio content or video content.
- Content Type Encoding – It defines the method used for encoding the message. Like 7-bit encoding, 8-bit encoding, etc.
- Content Id – It is used for uniquely identifying the message.
- Content description – It defines whether the body is actually image, video or audio.

# HyperText Transfer Protocol (HTTP)

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

#HTTP Transactions

The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.

1. **Request Message:** The request message is sent by the client that consists of a request line, headers, and sometimes a body.
2. **Response Message:** The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

#Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.

○ The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.

- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

#File transfer protocol FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Requirement of FTP

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP

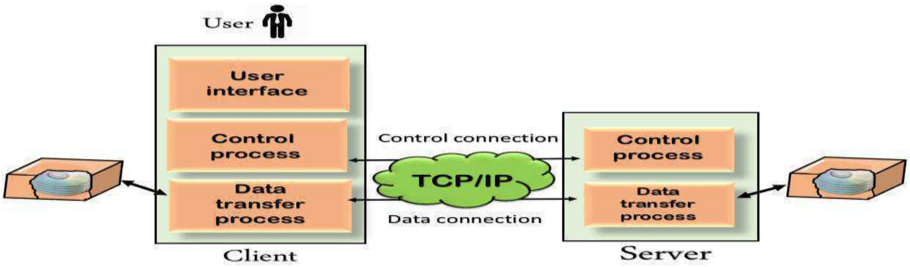


Fig. 2.9 Basic model of the FTP.

The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:

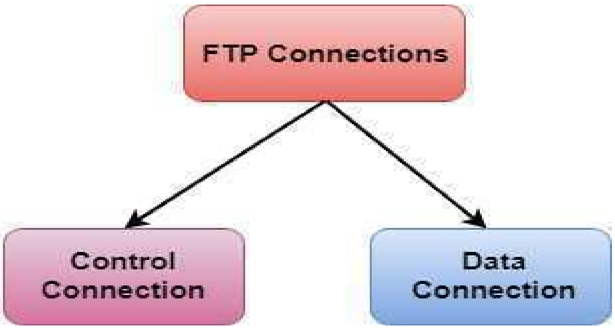


Fig. 2.10 Types of FTP

- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provide encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

Simple Network Management Protocol (SNMP):

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

SNMP Concept

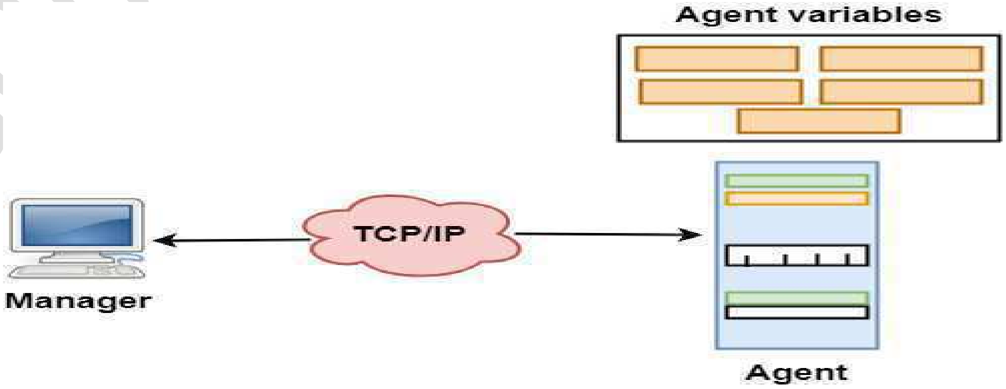


Fig. 2.11 SNMP Working Model

- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.

- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

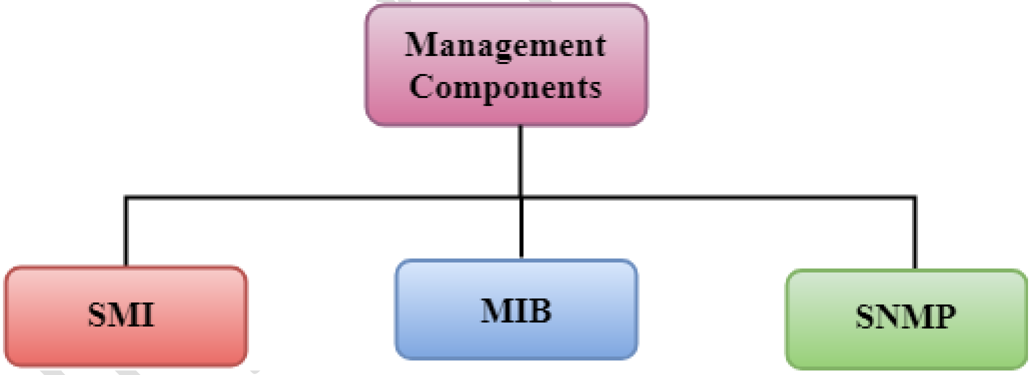


Fig. 2.12 Types of Management Components

SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

MIB

- The MIB (Management information base) is a second component for the network management.
- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.

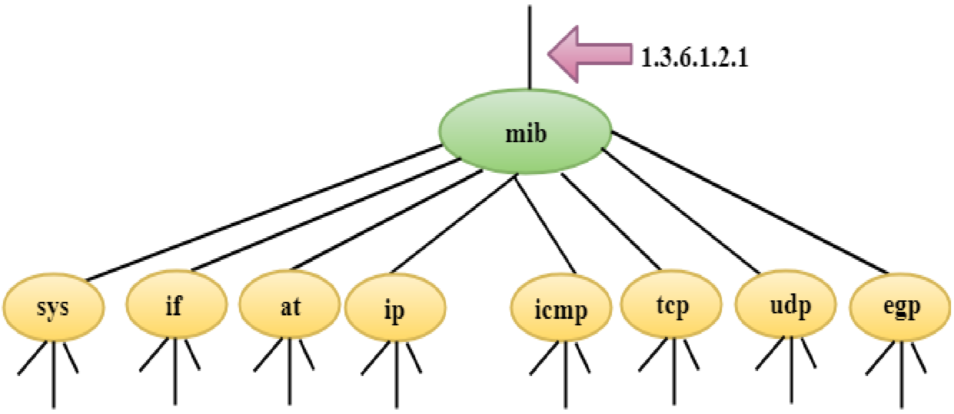


Fig. 2.13 MIB Architecture

SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.

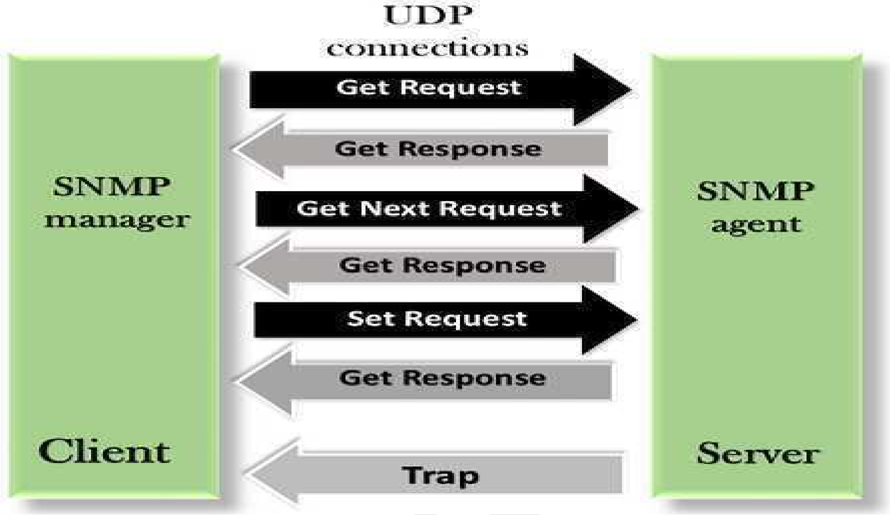


Fig.2.14 Simple Network Management Protocol

- **GetRequest:** The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.
- **GetNextRequest:** The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.
- **GetResponse:** The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.
- **SetRequest:** The SetRequest message is sent from a manager to the agent to set a value in a variable.
- **Trap:** The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

#DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.

- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP),is a technology that allowing you to make voice calls over a broadband Internet connection instead of a analog (regular) phone line. Some VoIP services allow you to call people using the same service, but others may allow you to call anyone. They can have a telephone number – including local, long distance, mobile, and international numbers or not. Some VoIP services only work over your computer or a special VoIP phone while other services allow you to use a traditional phone connected to a VoIP adapter.

Advantages of VoIP –

- Some VoIP services offer features and services that are not available with a traditional phone, or are available but only for an additional fee.
- Paying for both a broadband connection and a traditional telephone line can be avoided.
- Smoother connection than an analog signal can be provided.

Disadvantages of VoIP –

- Some VoIP services don’t work during power outages and the service provider may not offer backup power.
- Not all VoIP services connect directly to emergency services through emergency service numbers.
- VoIP providers may or may not offer directory assistance.

#Dynamic Host Configuration Protocol(DHCP)

Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

- Subnet Mask (Option 1 – e.g., 255.255.255.0)
- Router Address (Option 3 – e.g., 192.168.1.1)
- DNS Address (Option 6 – e.g., 8.8.8.8)
- Vendor Class Identifier (Option 43 – e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

These messages are given as below:

- **DHCP discover message** –
  This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long
- **DHCP offer message –**
  The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.
- **DHCP request message –**
  When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratitutous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.
- **DHCP acknowledgement message –**
  In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.
- **DHCP negative acknowledgement message –**
  Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.
- **DHCP decline –**
  If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.
- **DHCP release –**
  A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
- **DHCP inform –**
  If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Advantages – The advantages of using DHCP include:

- Centralized management of IP addresses

- Ease of adding new clients to a network
- Reuse of IP addresses reducing the total number of IP addresses that are required
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client
- The DHCP protocol gives the network administrator a method to configure the network from a centralised area.
- With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.

Disadvantages – Disadvantage of using DHCP is:

- IP conflict can occur