Application Layer

- It is the topmost i.e. seventh layer of OSI Model.
- It enables the user to access the network.
- It provides user interface & supports for services such as e-mail, file transfer, access to the world wide web.
- So it provides services to different user applications.

Functions of Application Layer

- **Mail Services:** This application provides various e-mail services.

- **File transfer & Access:** It allows users to access files in a remote host, to retrieve files from remote computer for use etc.

- **Remote log-in:** A user can log into a remote computer and access the resources of that computer.

- **Accessing the World Wide Web:** Most common application today is the access of the World Wide Web.

Contents

1. Domain Name System
   1. Name Space
   2. Server
   3. Queries
2. HTTP
3. FTP
4. Proxy
5. DHCP
6. E-mail
   1. SMTP
   2. POP
   3. IMAP

URL (Universal Resource Locator)

- URL is the abbreviation of **Uniform Resource Locator**
- **URL consist of following syntax**

protocol://host:port/path

1. Protocol : The *protocol* is the client/server program used to retrieve the document (eg: FTP, HTTP, HTTPS)
2. Host : Computer in which information is located
3. Path : the local path in which information is stores in the host
4. Port : The port number of the service used in the host

Example: http://www.google.com:80/index.html

URL is also called web address

1. Name Server (DNS- Domain Name System)

- All system communicate using IP(Numbers)
- Numbers are difficult to remember for human beings than name
  - Internet is very large there are millions of computer and servers
- Naming system is introduced(in 1983) for mapping of Host Name to IP address
- In DNS server, there is library procedure (program) called resolver that converts host name to IP
- **ICANN** (**Internet Corporation for Assigned Names and Numbers**) is responsible for managing the DNS in internet.
- Domain names are unique

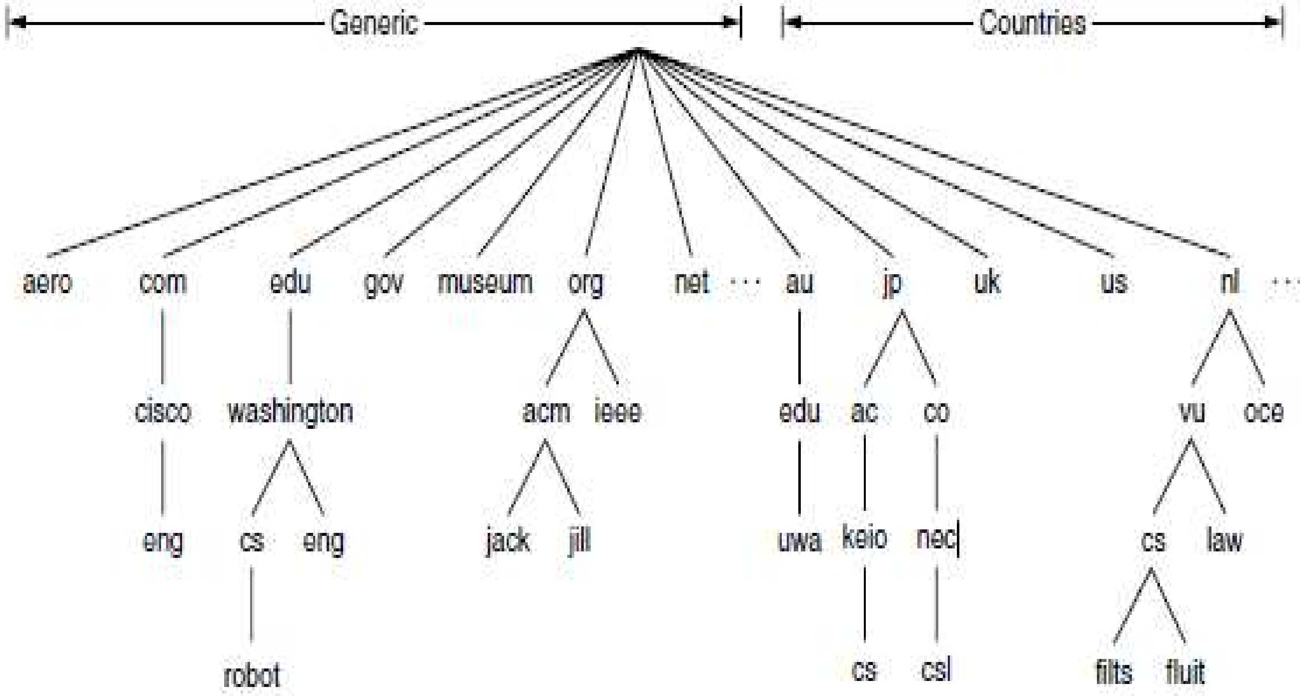
1.1. Name Spaces(Domain Name)

- Divided into 2 :
  1. Flat Structure
  2. Hierarchical Structure
- Hierarchical structure is used
  - Name space have tree structure
  - Example : www.xyz.com
  - *Here xyz.com is managed by central authority(ICANN) and www is name given by organization(here xyz)*

1.1.1. Domain Name Space

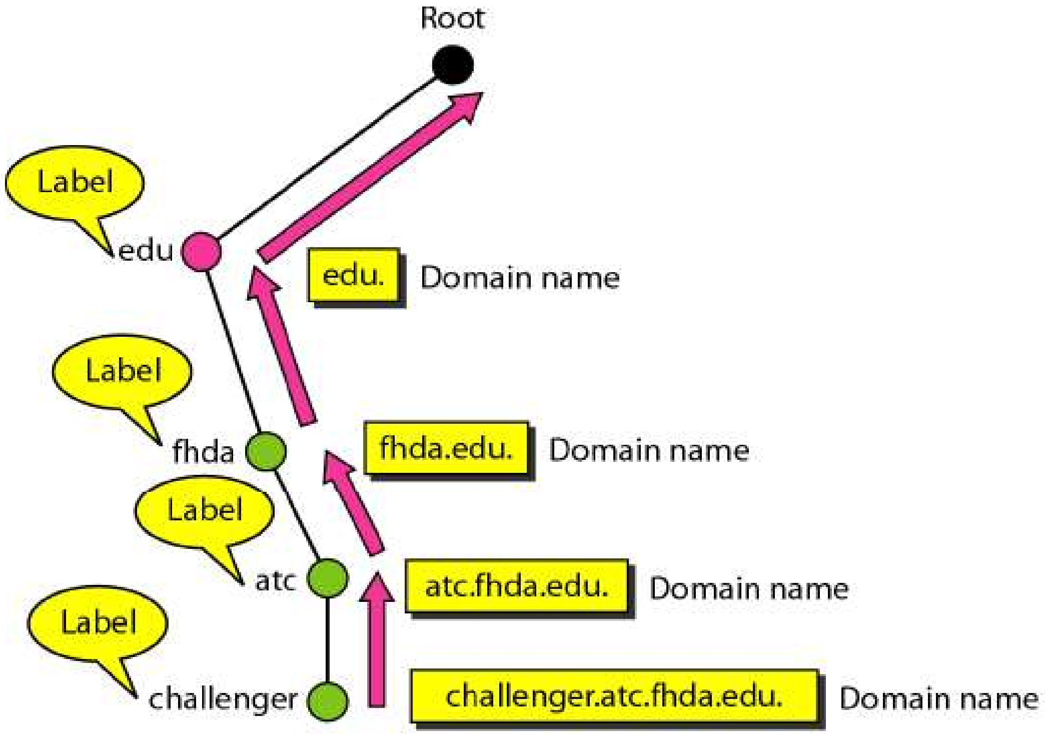
- Inverted Tree Structure, contains 0 to127 (128)levels
- 0 is root level
- Internet have nearly 250 **top-level domains**, where each domain covers many hosts
- Each domain is partitioned into **subdomains**, and these are further partitioned, and so on

com, edu, gov are example of top level domain



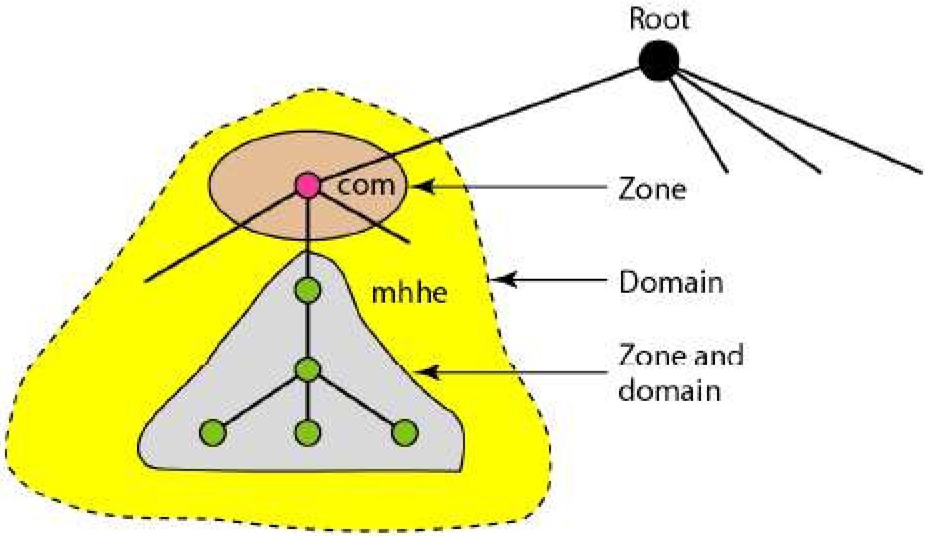
1.1.2. Domain Name

- All label is terminated by a null string(.), it is called a **FQDN (Fully Qualified Domain Name)**
- **Example:** *challenger.ate.tbda.edu.*
- Label is not terminated by a null string, it is called a **PQDN (Partially Qualified Domain Name)**
- A PQDN starts from a node, but it does not reach the root
- **Example :** *challenger.ate.tbda.edu*
- NB: **.(dot)** Is called root server



1.1.3. Zone

- Zone will keep track of all nodes in domain and all sub-domains under the domain.



1.2. Servers

- Root Server
  - A root server is a server whose zone consists of the whole tree
  - A root server usually does not store any information about domains but delegates its authority to other servers
- DNS defines two types of servers

1. Primary Server

- A primary server is a server
  - That stores a file about the zone for which it is an authority
  - It is responsible for **creating, maintaining, and updating the zone file**

2. Secondary Server
   - A secondary server is a server that **transfers the complete information about a zone** from another server (primary or secondary) and stores the file on its local disk

1.3. Query

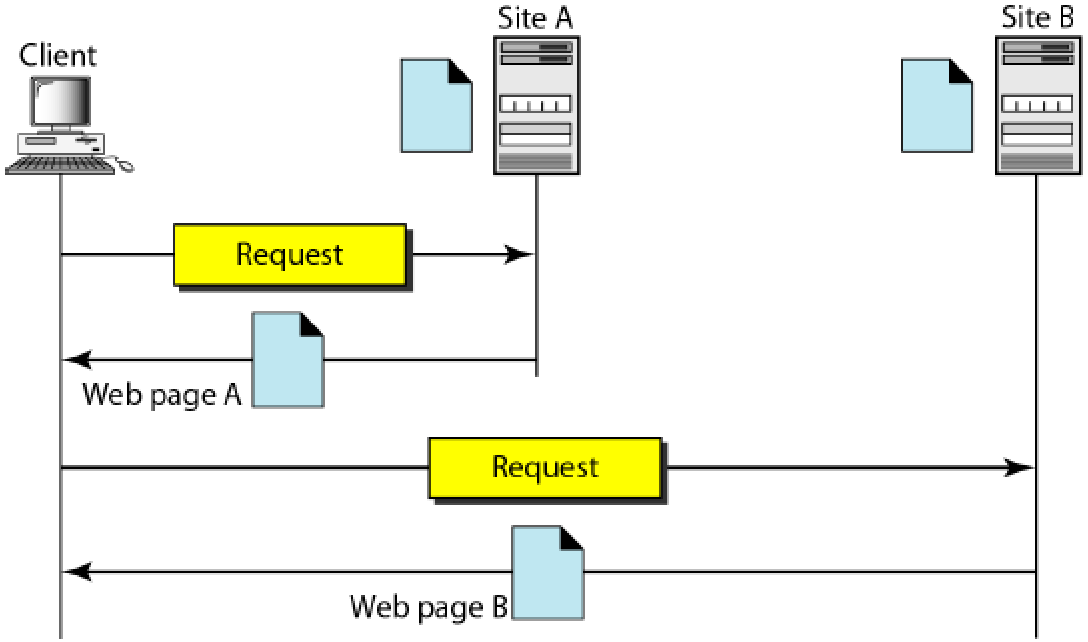
- DNS has two types of messages

1. **Query** - sent by DNS client to server, **Query message consists** of a header and question records
2. **Response** – sent by DNS server to client, **Response message consists** of a header, question, records, answer records, authoritative records, and additional records
   - Query is a question to the server, Client ask about the **IP address** of the mentioned **URL**
   - **Response** is answer to the question provided by client from server, i.e. it sent information (IP address) of the mentioned URL

2. HTTP-(Hyper Text Transfer Protocol)

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web(WWW)
- It is similar to FTP because it transfers files and uses the services of TCP.
- It uses only one TCP connection
- HTTP uses the services of TCP on well-known **port 80**
- Accessing of web page is based on URL

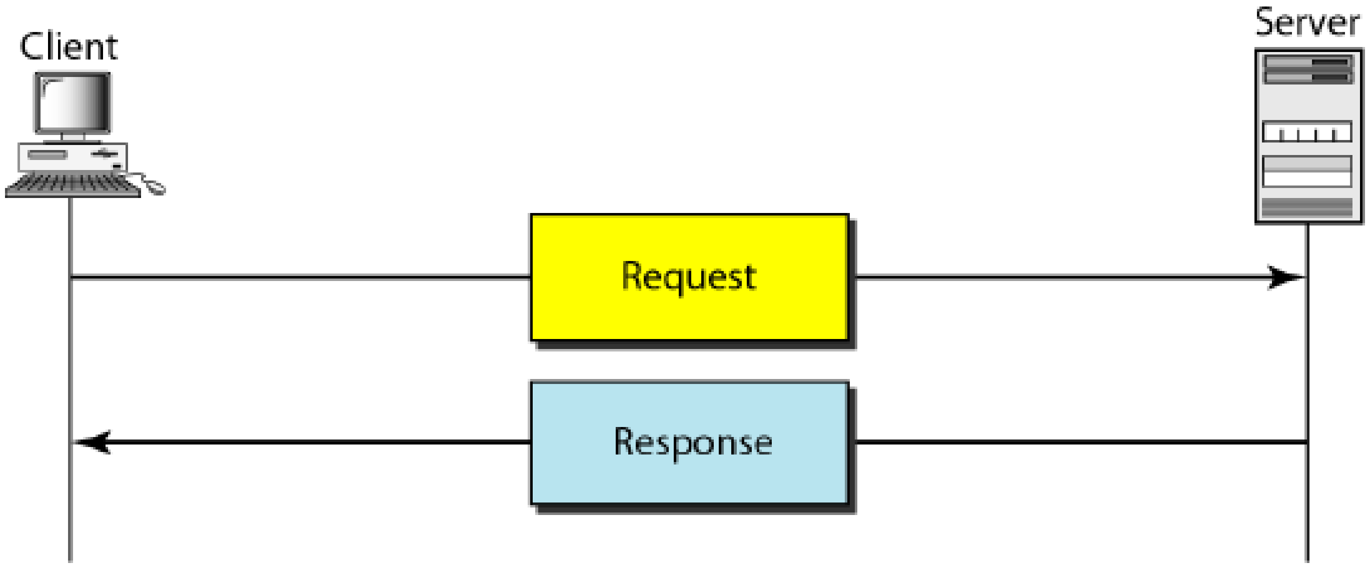
2.1. WWW Architecture



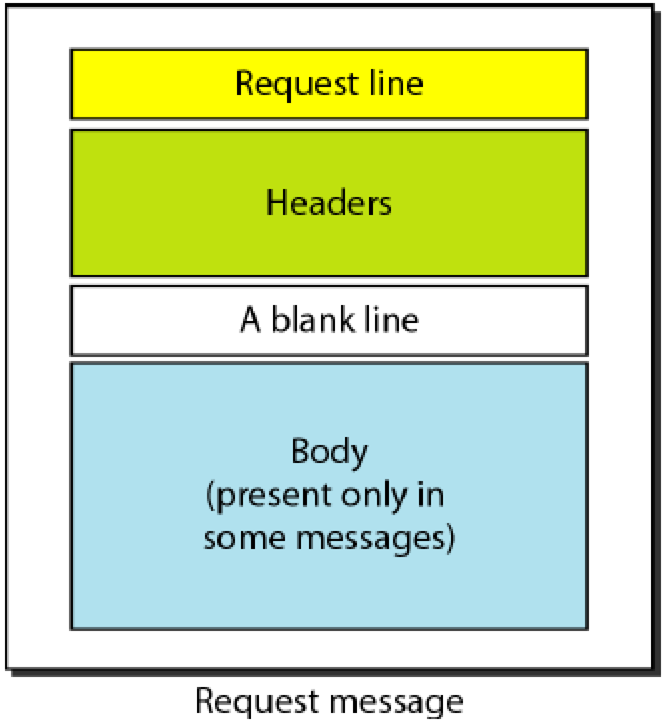
2.2. HTTP Transaction

- HTTP transaction between the client and server
- There are 2 transaction messages
- Request (sent from client to server for requesting a Page or other resource)
- Response (sent from server to client)

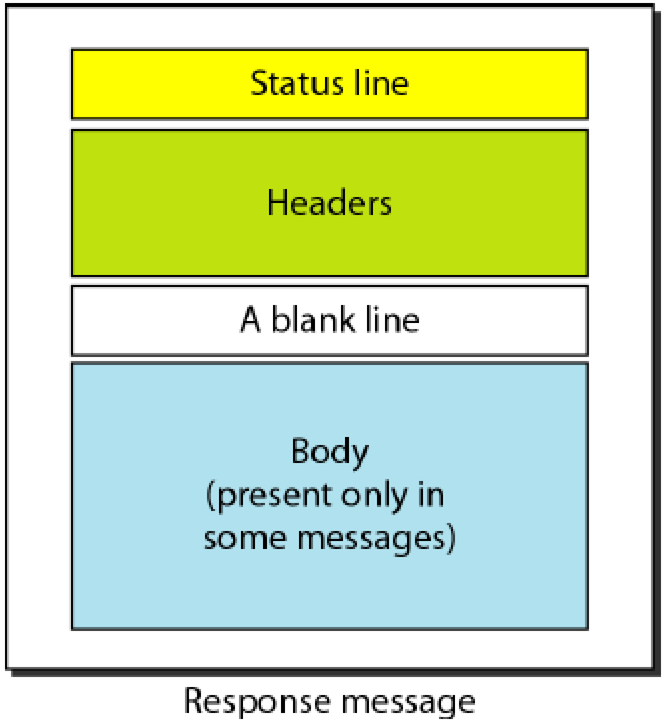
2.2. HTTP Transaction Figure



2.2.1 Message Format



Request message

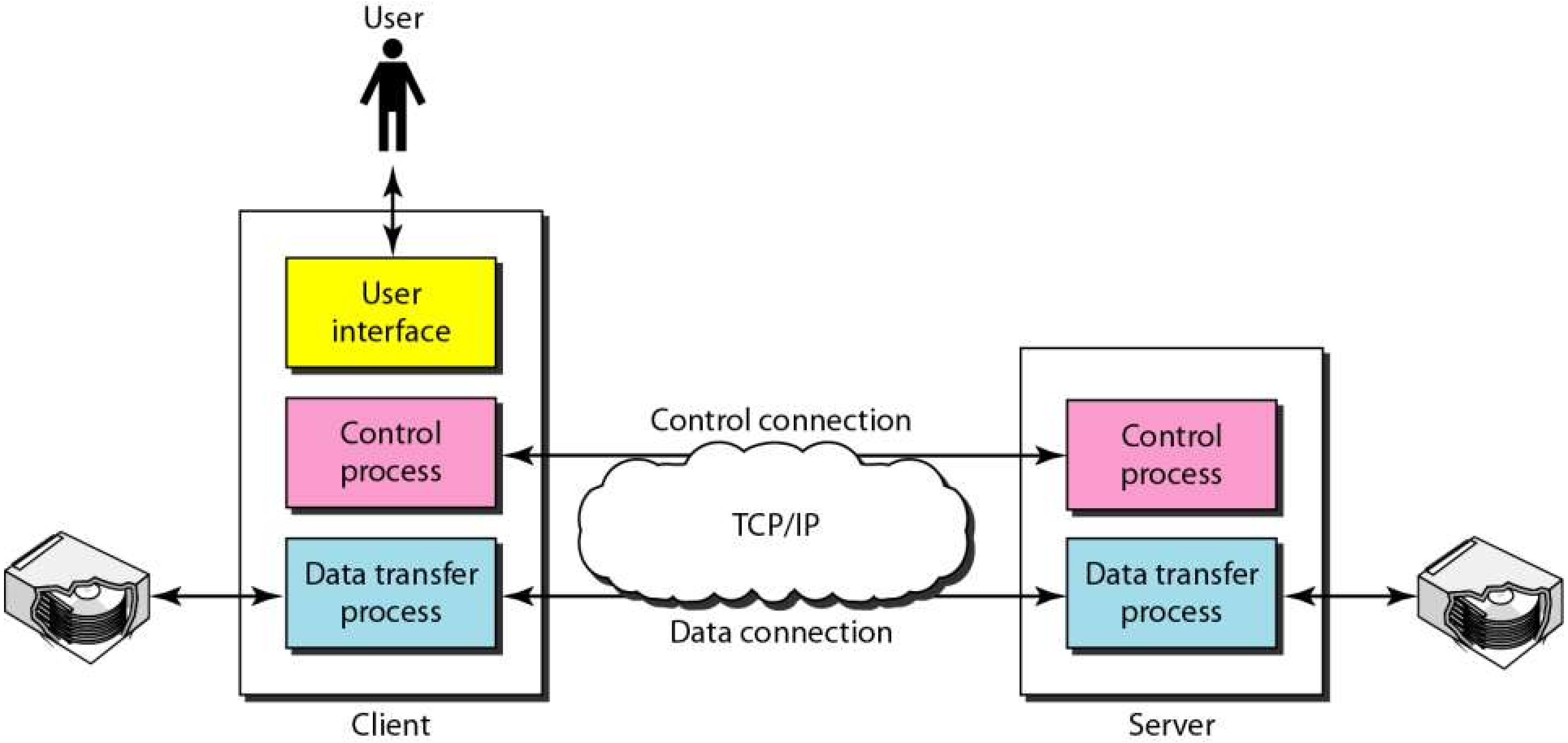


Response message

3. FTP (File Transfer Protocol)

- File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another
- FTP establishes two connections between the hosts
- One connection is used for data transfer, the other for control information (commands and responses)
- Separation of commands and data transfer makes FTP more efficient
- FTP uses **two** well-known TCP ports: **Port 21** is used for the control connection, and **port 20** is used for the data connection.

3.1. FTP Architecture



3.2. FTP Working

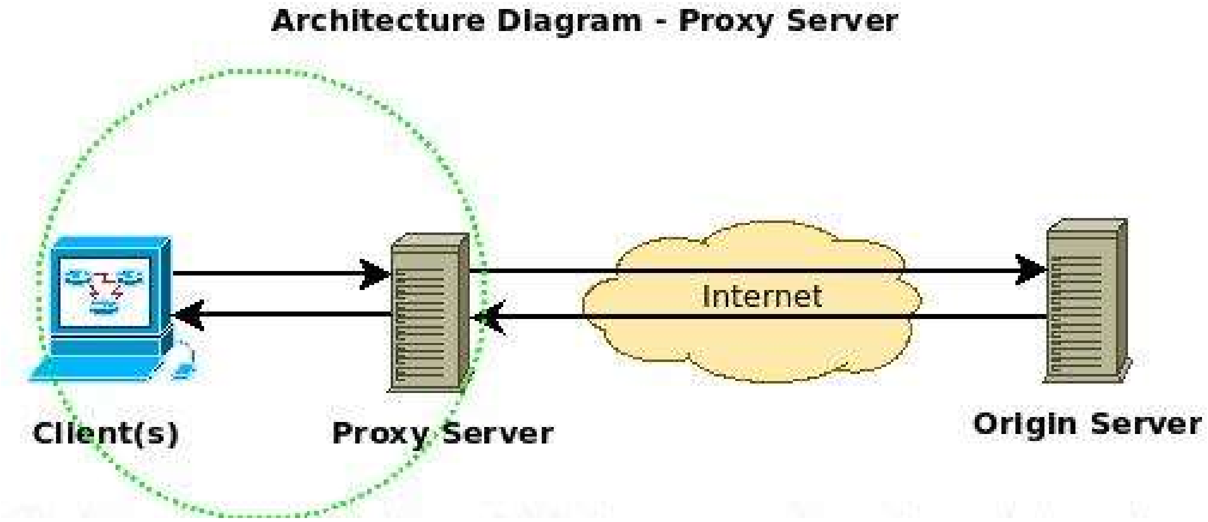
- FTP uses Transmission Control Protocol (TCP) for reliable network communication by establishing a session before initiating data transfer
- FTP client send command/ request for connection to FTP server establishing connection(Port 21)
- FTP server Responds to the commands about the status wheatear connected/ not connected (Port 21)
- FTP Client connect to FTP server using control connection i.e. using port 21
- After establishing connection port 20 is used for data transfer

4. Proxy Server

- A proxy server is a computer that keeps copies of responses to **recent requests**
- The HTTP client sends a request to the proxy server
- The proxy server checks its cache, If the response is not stored in the cache, the proxy server sends the request to the corresponding server
- Incoming responses are sent to the proxy server and stored for future requests from other clients
- The proxy server **reduces the load on the original server**, decreases traffic, and improves latency

4. Proxy Server

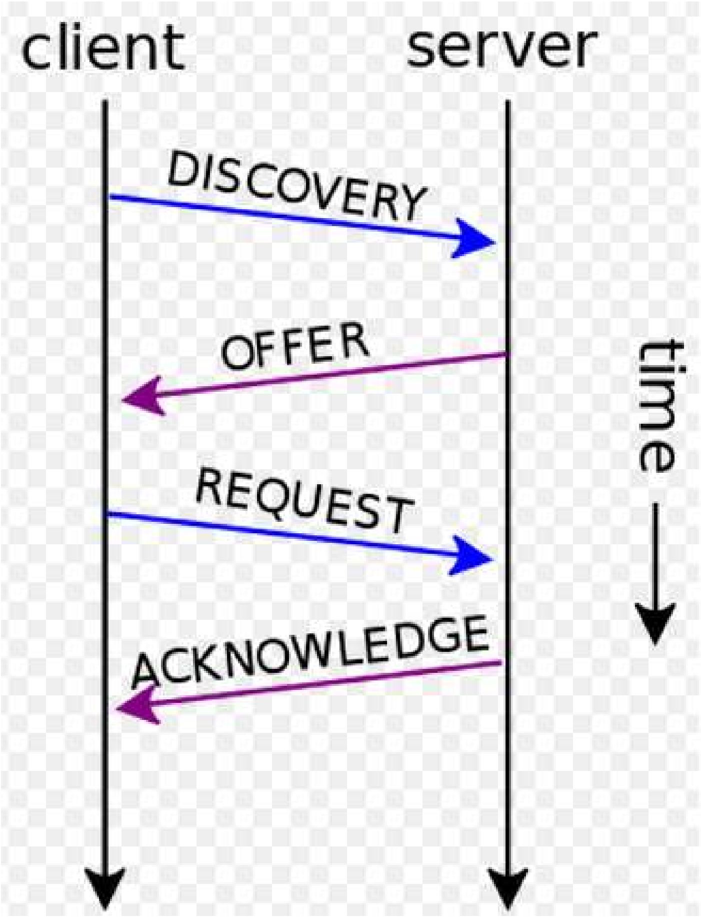
- However, to use the proxy server, the client must be configured to access the proxy instead of the target server



5. DHCP(Dynamic Host Configuration Protocol)

- Two possible way for configuring IP are:
  1. Manually
  2. Dynamically (DHCP)
- DHCP is service that provide IP addresses.
- Server that runs DHCP service is DHCP servers.
- Client that uses DHCP server for IP configuration is DHCP clients.
- DHCP server uses UDP port 67
- DHCP client uses UDP port 68

5.1. DHCP Operation



5.1.1. DHCP Discover Packet

- Sent by DHCP client to DHCP server(Broadcasting)
- DHCP client ***(****computer or device which wants IP****)*** broadcast broadcasts a request for an IP address on its network. It does this by using a DHCP DISCOVER packet
- Packet must reach the DHCP server
- A DHCP client may also request its last-known IP address with discover packet
- DHCP discover packet is for checking weather DHCP server is available in network and IP address lease request

5.1.2. DHCP Offer Packet

- Sent by DHCP server to DHCP client (Unicasting)
- When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client
- This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer

5.1.3. DHCP Request Packet

- Sent by DHCP client to DHCP servers (Broadcasting)
- In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address.
- A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer
- Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.
- When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

5.1.4. DHCP Acknowledgement Packet

- Sent by DHCP servers to DHCP client (Unicasting)
- When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase.
- The acknowledgement phase involves sending a DHCP ACK packet to the client.
- This packet includes the lease duration and any other configuration information that the client might have requested.
- At this point, the IP configuration process is completed

6. E-mail

- Electronic mail, or more commonly **email**, used to communicate with different users in internet
- Email uses following protocols for storing & delivering messages, They are :
  1. SMTP (Simple Mail Transfer Protocol)
  2. POP (Post Office Protocol)
  3. IMAP (Internet Message Access Protocol)

6. E-mail

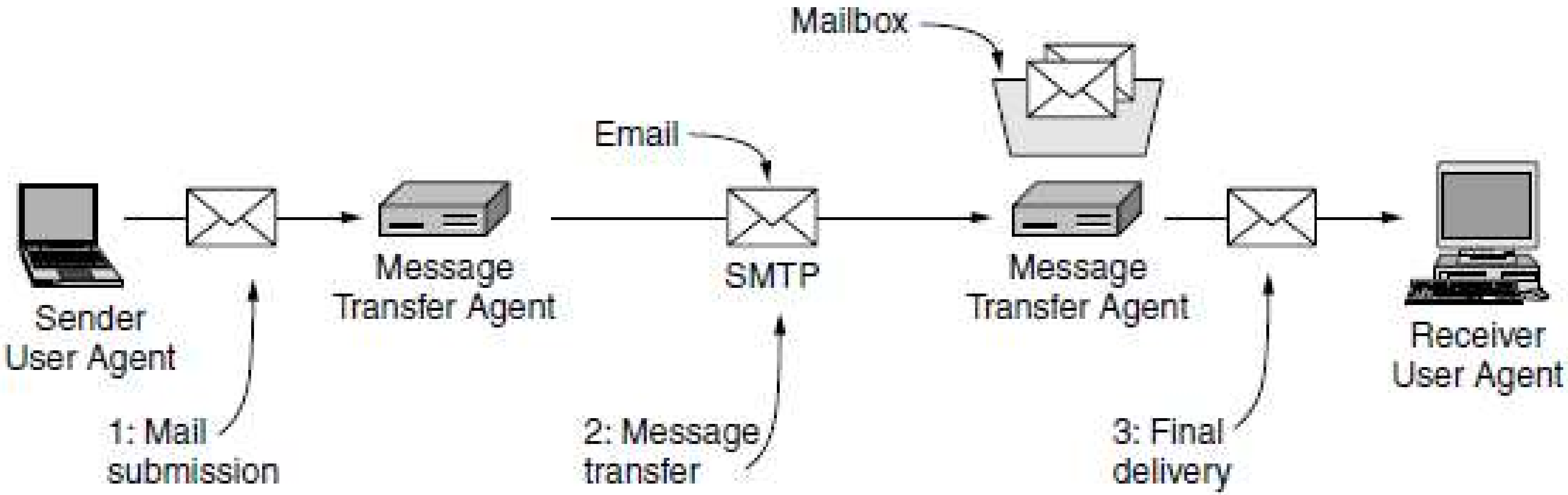
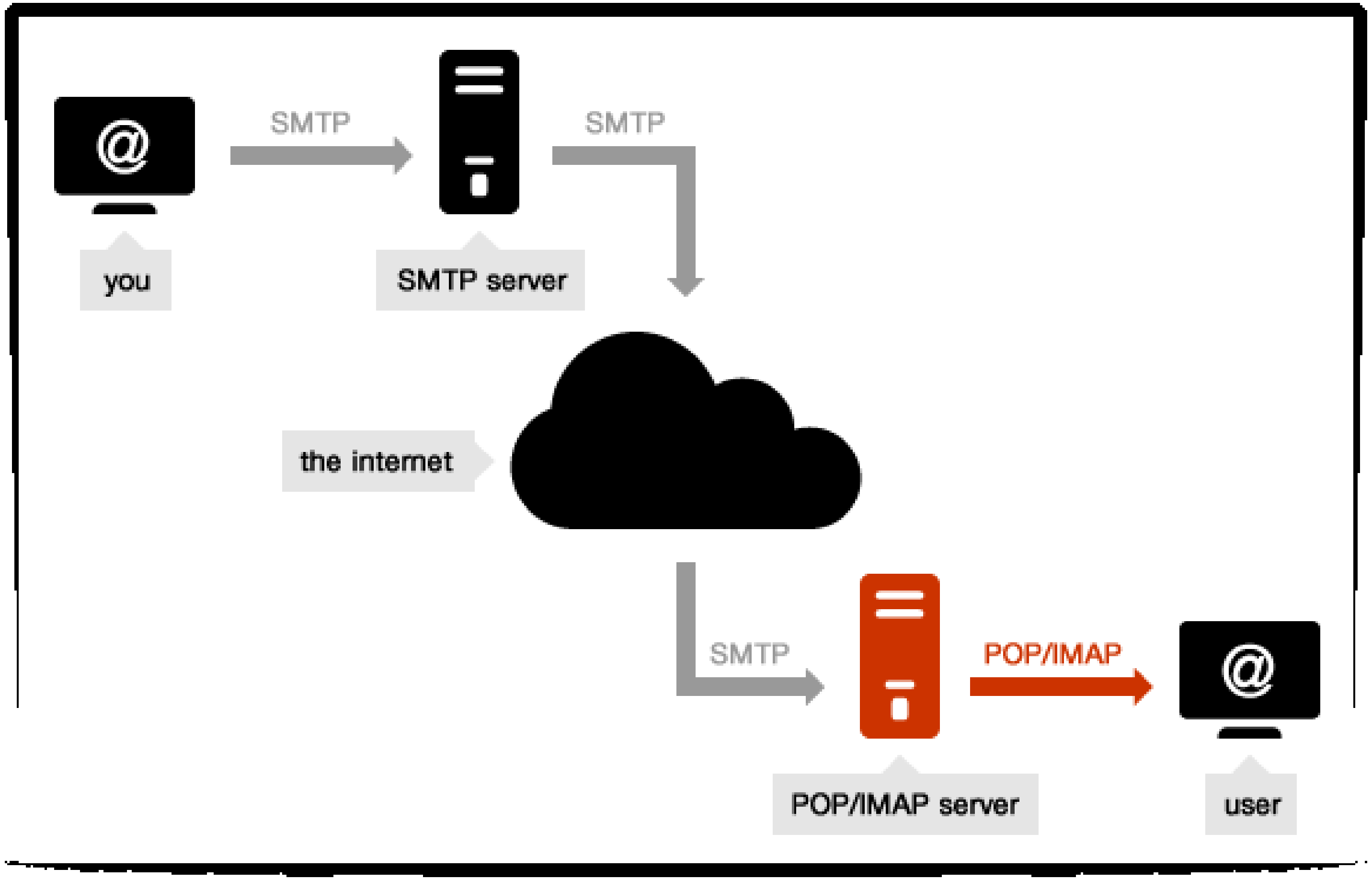


Figure Architecture of the email system.

6. E-mail

- Email consists of two kinds of subsystems
  1. **Mail User Agents (also called MUA/email client programs)**: which allow people to read and send email (Ex: Outlook)
  2. **Message Transfer Agents(also called MTA/ Email Server)** : which move the messages from the source to the destination (Ex: Gmail Server)
- Act of sending new messages into the mail system for delivery is called **Mail submission (Email Client to Email Sever)**
- The Process of transferring mail from one MTA to another (Ex : from gmail to yahoo server) is called **Message Transfer**
- **Mailboxes** store the email that is received for a user

6. E-mail (Working all Protocols)



6.1. SMTP (Simple Mail Transfer Protocol)

- Message transfer form originator to the recipient mailbox is done with SMTP
- It uses TCP well known port 25
- SMTP server accepts incoming connections, subject to some security checks, and accepts messages for delivery
- If a message cannot be delivered, an error report containing the first part of the undeliverable message is returned to the sender
- Email is submitted by a mail client **(MUA, mail user agent)** to a mail server (**MSA, mail submission agent)** using SMTP on TCP port 587
- **MSA** delivers the mail to its mail transfer agent **MTA**

6.1.1. Features of SMTP

- SMTP supports sending of email only It cannot retrieve (deliver to user) messages from a remote server on demand
- SMTP provides system for sending message to same (or different) servers (gmail **to** gmail **/** gmail **to** yahoo)
- SMTP provide a mail exchange between users on same (or different) server
- SMTP supports:
    1. Sending a message to one or more recipients
    2. Sending message that includes text, voice, video or graphics
    3. Sending message to users on other network

6.2. POP (Post Office Protocol)

- Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection
- POP has been developed through several versions, with version 3 (POP3) being the last standard
- E-mails are downloaded from the server's mailbox to your computer
- No copy of Email will be kept in mailbox after downloading the email
- E-mails are available when you are not connected

6.2.1. POP Working

- Working of POP servers is as following steps:
  1. Connect to server
  2. Retrieve all mail
  3. Store locally as new mail
  4. Delete mail from server*
  5. Disconnect

** Deletion of mail is default setting , However user can change the settings to keep the copy of email in mail box*

6.2.2.Features of POP

- POP is a much simpler protocol, making implementation easier
- POP mail moves the message from the email server onto your local computer, although there is usually an option to leave the messages on the email server as well
- POP treats the mailbox as one store, and has no concept of folders
- POP protocol requires the currently connected client to be the only client connected to the mailbox
- When POP retrieves a message, it receives all parts of it

6.2.3. Advantages of POP

- Advantages are:

1. Mail stored locally, i.e. always accessible, even without internet connection
2. Internet connection needed only for sending and receiving mail
3. Saves server storage space
4. Option to leave copy of mail on server

6.3. IMAP (Internet Message Access Protocol)

- Protocols that is used for final delivery is **IMAP**
- **IMAP** is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection
- IMAP provides mechanisms for storing messages received by SMTP in a mailbox
- IMAP server stores messages received by each user until the user connects to download and read them using an email clients

** Now a days IMAP replaced POP in all E-mail services*

6.3.1. IMAP Working

- Working of IMAP servers is as following steps:
  1. Connect to server
  2. Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails
  3. Process user edits, *e.g. marking email as read, deleting email etc.*
  4. Disconnect

6.3.2 Features of IMAP

- Connected and disconnected modes of operation (Faster Operation)
- Multiple clients simultaneously connected to the same mailbox
- Access to message parts and partial fetch of messages (No need for complete message to be displayed only **subject / user name** can be retrieved)
- Provides message state information (**Message states are :** read / unread / replied / forwarded)
- Provides multiple mailboxes on the server (create new mail boxes and copy form one to another)
- Provides mechanisms for server-side searches

6.3.3. IMAP Advantage

Advantages

1. Mail stored on remote server, i.e. accessible from multiple different locations
2. Internet connection needed to access mail
3. Faster overview as only headers are downloaded until content is explicitly requested
4. Mail is automatically backed up if server is managed properly
5. Saves local storage space
6. Option to store mail locally

1. Network Management

- **Network Management** is defined as **monitoring, testing, configuring,** and **troubleshooting** network components to meet a set of requirements defined by an organization/user
- Network Management system can be divided into five broad categories:
  1. Configuration Management
  2. Fault Management
  3. Performance Management
  4. Security Management
  5. Accounting Management

1.1 Configuration Management

- Configuration management system must know, at any time, the status of each entity *(hardware/software/user)* and its relation to other entities
- Configuration management can be subdivided into two parts
  1. **Reconfiguration**, which means adjusting the network components and features, can be a daily occurrence in a large network. There are three types of reconfiguration: **hardware reconfiguration, software reconfiguration, and user-account reconfiguration**
  2. **Documentation**, The original network configuration and each subsequent change must be **recorded** properly. This means that there must be documentation for **hardware, software, and user accounts**

1.2. Fault Management

- Proper operation of the network depends on the proper operation of each component individually and in relation to each other
- **Fault management** handles this issue weather individual component or relation between component is working properly or not.
- Fault management system has two subsystems:
  1. **Reactive fault management system** is responsible for detecting, isolating, correcting, and recording faults. It handles short-term solutions to faults
  2. **Proactive fault management** tries to prevent faults from occurring. Although this is not always possible, some types of failures can be predicted and prevented

1.3. Performance Management

- **Performance management,** which is closely related to fault management, tries to monitor and control the network to ensure that it is running as efficiently as possible
- Performance management tries to quantify performance by using some measurable quantity such as
    1. Capacity : he performance management system must ensure that it is not used above this capacity
    2. Traffic : Traffic can be measured in two ways: **internally and externally**. **Internal traffic** is measured by the number of packets (or bytes) traveling inside the network. **External traffic** is measured by the exchange of packets (or bytes) outside the network
    3. Throughput : Performance management monitors the throughput to make sure that it is not reduced to unacceptable levels
    4. Response Time : Response time is normally measured from the time a user requests a service to the time the service is granted

1.4. Security Management

- **Security management** is responsible for controlling access to the network based on the predefined policy
- Security management is done with help of Cryptography, Digital signature, IPSec, VPN

1.5. Accounting Management

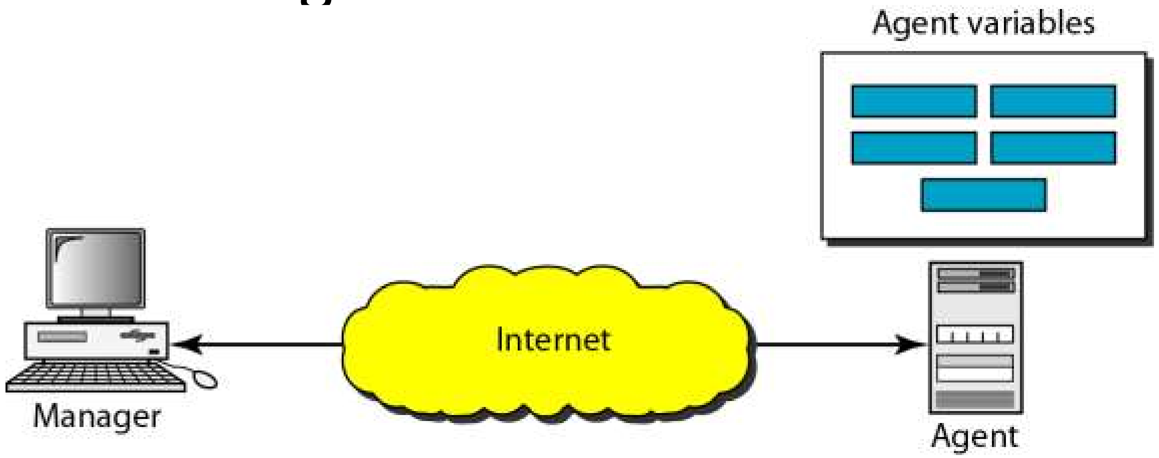
- Accounting management is the control of users access to network resources through charges
- Under accounting management, individual users, departments, divisions, or even projects are charged for the services they receive from the network
- Organizations use an accounting management system for the following reasons:
    1. It prevents users from monopolizing limited network resources
    2. It prevents users from using the system inefficiently
    3. Network managers can do short- and long-term planning based on the demand for network use

2. SNMP

- **Simple Network Management Protocol (SNMP)** is a framework for managing devices in network
- It provides a set of fundamental operations for **monitoring** and **maintaining** network
- SNMP uses the concept of **manager** and **agent**
- SNMP is an application-level protocol in which a few manager stations control a set of agents
- ***Manager***, usually a host, **controls** and **monitors** a set of ***agents***, usually routers

2.1. SNMP Concepts

- Management is achieved through simple interaction between a **manager** and an **agent**
- **Agent** keeps performance information in a database
- **Manager** has access to the values in the database
- The manager can fetch and compare the values of these two variables to see if the router is congested or not

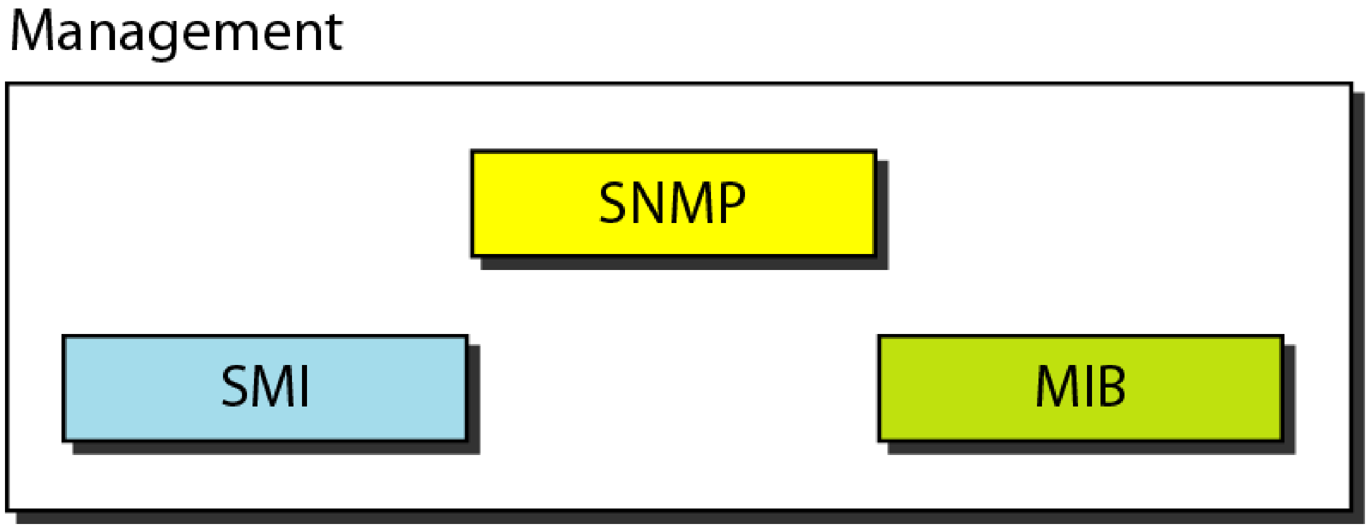


2.1. SNMP Concepts

- Management with SNMP is based on three basic ideas:
  1. A manager checks an agent by requesting information that reflects the behaviour of the agent.
  2. A manager forces an agent to perform a task by resetting values in the agent database.
  3. An agent contributes to the management process by warning the manager of an unusual situation
- **SNMP managed network** consists of three key components:
  1. Managed device → Device which is managed by **SNMP also called network elements**
  2. Agent → software which runs on managed devices
  3. Network management system (NMS) → software which runs on the manager

2.2. SNMP Components

- For management tasks SNMP uses two other protocols:
  1. Structure of Management Information (SMI)
  2. Management Information Base (MIB)
- Management on the Internet is done through the cooperation of the three protocols **SNMP, SMI**, and **MIB**



2.2.1. Role of SNMP

- SNMP has some very specific roles in network management. They are:
  1. Defines the format of the packet to be sent from a manager to an agent and vice versa
  2. Interprets the result and creates statistics
  3. The packets exchanged contain the object (variable) names and their status (values)
  4. SNMP is responsible for reading and changing these values

2.2.2. Role of SMI

- SMI functions are:
  1. To name objects
  2. To define the type of data that can be stored in an object
  3. To show how to encode data for transmission over the network
- SMI does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values

2.2.3. Role of MIB

- MIB creates
  1. A set of objects defined for each entity similar to a database
  2. MIB creates a collection of named objects, their types
  3. Creates objects relationships to each other in an entity to be managed
- MIB must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object