# UNIT-V

## Application Layer

# Introduction to Application Layer

- The application layer is the topmost layer of the OSI model and the TCP/IP model.
- In TCP/IP model, the application layer is formed by combining the top three layers, i.e., the application layer, the presentation layer, and the session layer.
- An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network.
- It is the layer closest to the end-user, implying that the application layer and the end-user can interact directly with the software application.

# Services Provided by the Application Layer

The application provides the following services.

- The application layer guarantees that the receiver is recognized, accessible, and ready to receive data from the sender.
- It enables authentication between devices for an extra layer of network security.
- It determines the protocol and data syntax rules at the application level.
- The protocols of the application layer also define the basic syntax of the message being forwarded or retrieved.
- It also checks whether the sender's computer has the necessary communication interfaces, such as an Ethernet or Wi-Fi interface.
- Finally, the data on the receiving end is presented to the user application.

# Application Layer Protocols

- The various protocols used in the application layer make the communication between the sender and receiver **faster, efficient, reliable, and safe.** The protocols are:

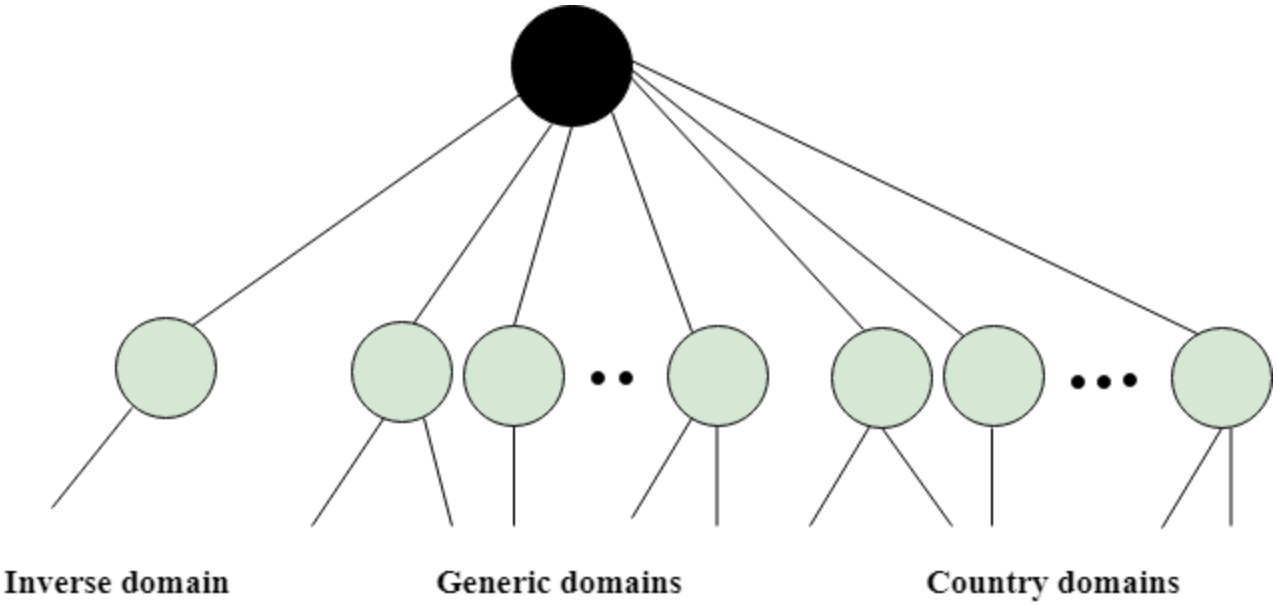
1. HTTP
2. DNS
3. FTP
4. TFTP
5. EMail
6. SNMP
7. BOOTP

# Domain Name System(DNS)

- 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.

# Domain Name System(DNS)

- 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.



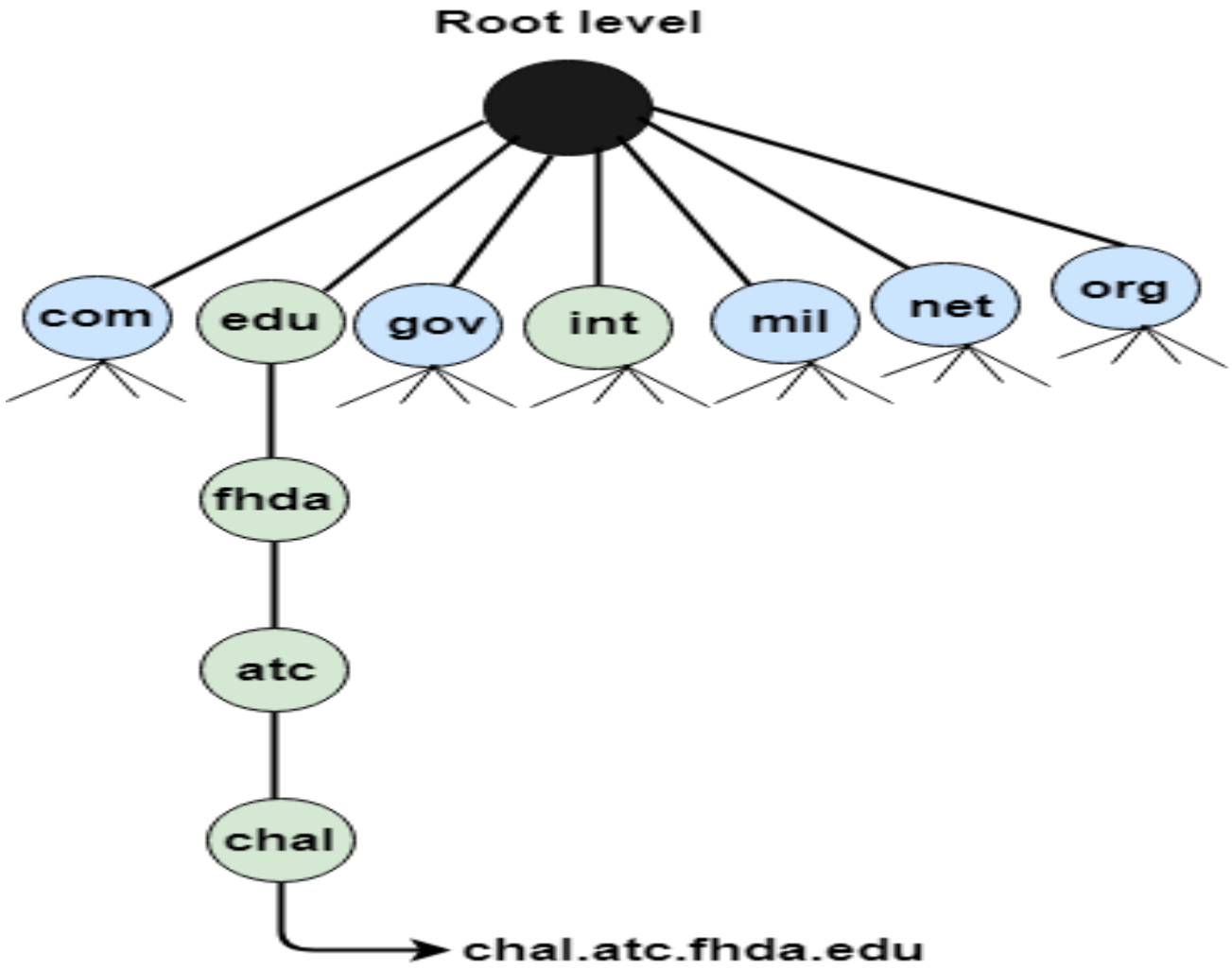
# Domain Name System(DNS)

**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.

| Label | Description |
|---|---|
| aero | Airlines and aerospace companies |
| biz | Businesses or firms |
| com | Commercial Organizations |
| coop | Cooperative business Organizations |
| edu | Educational institutions |
| gov | Government institutions |
| info | Information service providers |
| int | International Organizations |
| mil | Military groups |
| museum | Museum & other nonprofit organizations |
| name | Personal names |
| net | Network Support centers |
| org | Nonprofit Organizations |
| pro | Professional individual Organizations |

# Domain Name System(DNS)



# Domain Name System(DNS)

**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.

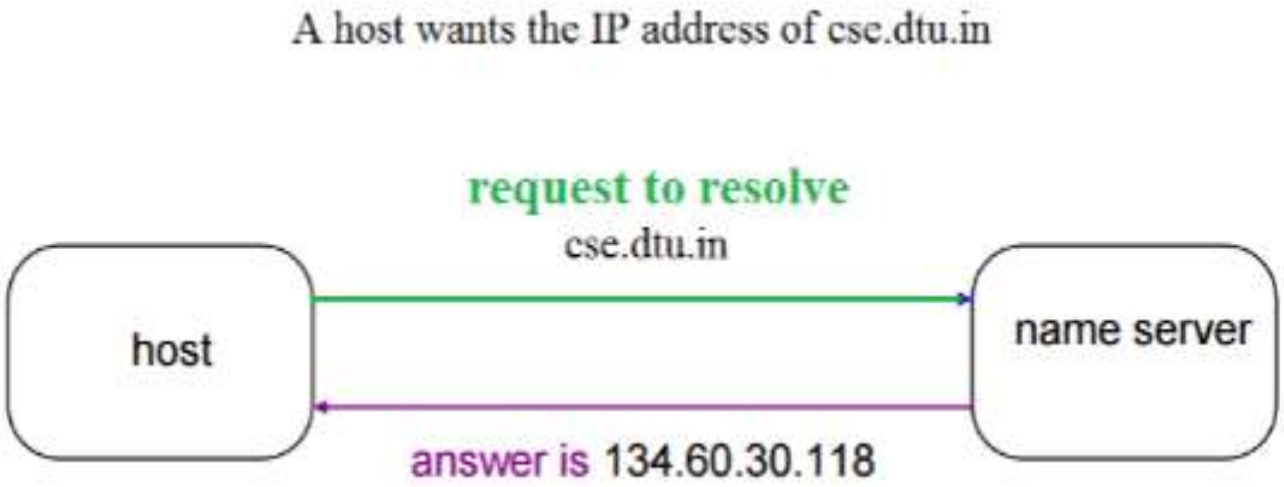
# Domain Name System(DNS)

It is very difficult to find out the IP address associated to a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delay for that to happen organization of database is very important.

- **DNS record:** Domain name, IP address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
- **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
- **Name server:** It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

# Domain Name System(DNS)

**Name to Address Resolution:**



# Domain Name System(DNS)

**Hierarchy of Name Servers**

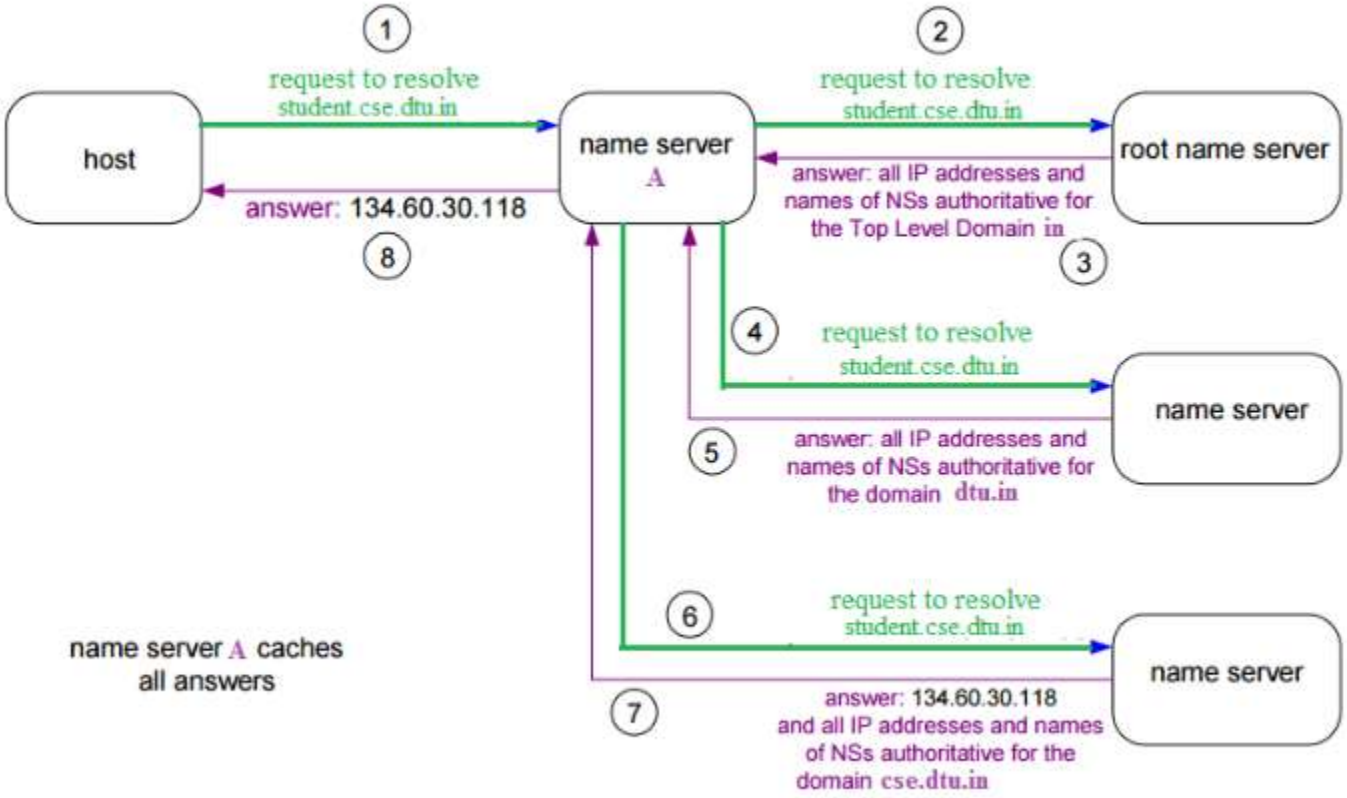
- **Root name servers:** It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.

- **Top level domain (TLD) server:** It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.

- **Authoritative name servers** are the organization's DNS server, providing authoritative host Name to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative IP address.

# Domain Name System(DNS)

**Domain Name Server:**



# Domain Name System(DNS)

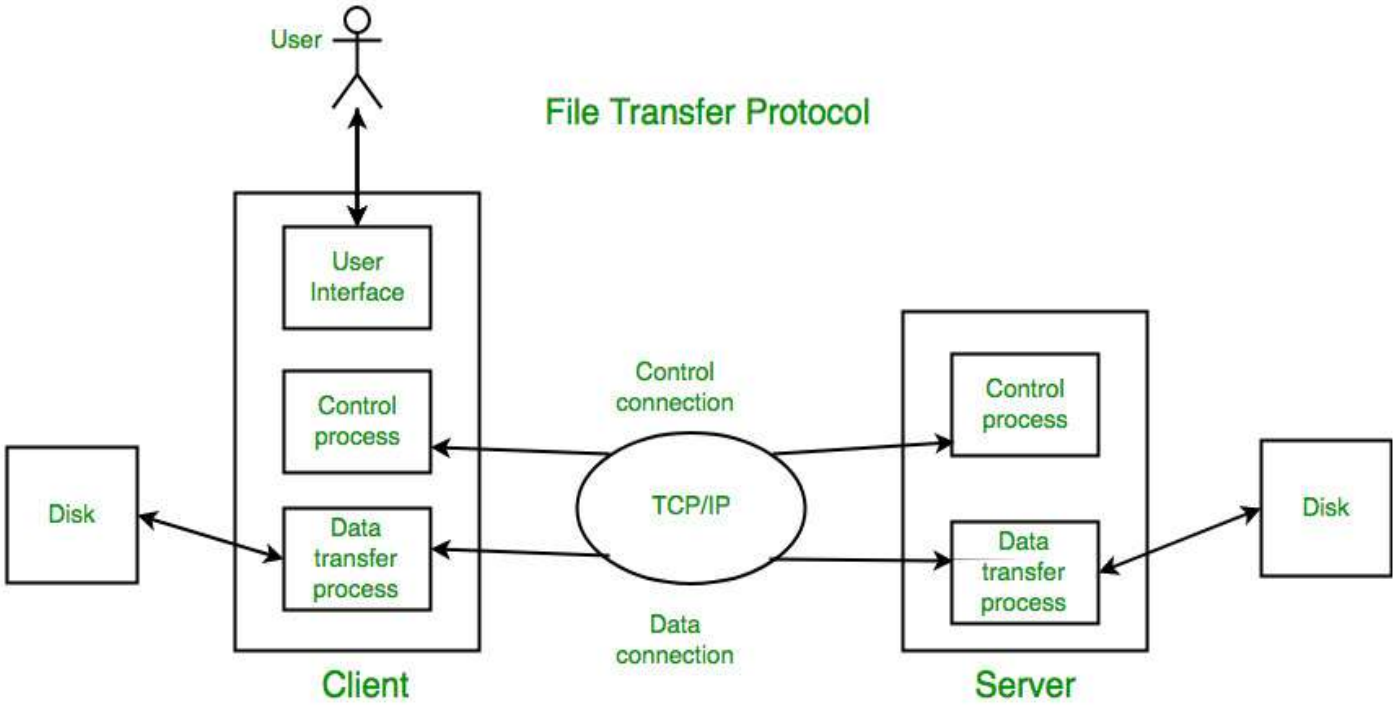
- The client machine sends a request to the local name server, which , if local name server does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an top-level domain (TLD) or authoritative name server.

- The root name server can also contain some host Name to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is.

- So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

# File Transfer Protocol(FTP)

- File Transfer Protocol(FTP) is an application layer protocol that moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.



# File Transfer Protocol(FTP)

**Control connection:**

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

**Data Connection:**

- For sending the actual file, FTP makes use of a data connection.
- A data connection is initiated on port number 20. FTP sends the control information out-of-band as it uses a separate control connection.
- Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

# File Transfer Protocol(FTP)

**FTP Session:**

- When an FTP session is started between a client and a server, the client initiates a control TCP connection with the server-side. The client sends control information over this.
- When the server receives this, it initiates a data connection to the client-side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session.
- As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.

**Data Structures:**

FTP allows three types of data structures :

- **File Structure –** In file structure, there is no internal structure and the file is considered to be a continuous sequence of data bytes.
- **Record Structure –** In record structure, the file is made up of sequential records.
- **Page Structure –** In page structure, the file is made up of independent indexed pages.

# File Transfer Protocol(FTP)

**FTP Commands :**

***USER –*** This command sends the user identification to the server.
***PASS –*** This command sends the user password to the server.
***CWD –*** This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.
***STOR –*** This command causes to store of a file into the current directory of the remote host.
***LIST –*** Sends a request to display the list of all the files present in the directory.
***ABOR –*** This command tells the server to abort the previous FTP service command and any associated transfer of data.
***QUIT –*** This command terminates a USER and if file transfer is not in progress, the server closes the control connection.

# File Transfer Protocol(FTP)

**FTP Replies:**

**200** Command okay.
**530** Not logged in.
**331** User name okay, need a password.
**225** Data connection open; no transfer in progress.
**221** Service closing control connection.
**551** Requested action aborted: page type unknown.
**502** Command not implemented.
**503** Bad sequence of commands.
**504** Command not implemented for that parameter.

# File Transfer Protocol(FTP)

**Advantages of FTP(File Transfer Protocol):**

- Speed is one of the advantages of FTP(File Transfer Protocol).
- File sharing also comes in the category of advantages of FTP in this between two machines files can be shared on the network.
- Efficiency is more in FTP.

**Disadvantages of FTP(File Transfer Protocol):**

- File size limit is the drawback of FTP only 2 GB size files can be transferred.
- Multiple receivers are not supported by the FTP.
- FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
- FTP is unsecured we use login IDs and passwords making it secure but they can be attacked by hackers.

# 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.

# Trivial File Transfer Protocol(TFTP)

**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 is 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.

# Trivial File Transfer Protocol(TFTP)

**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.

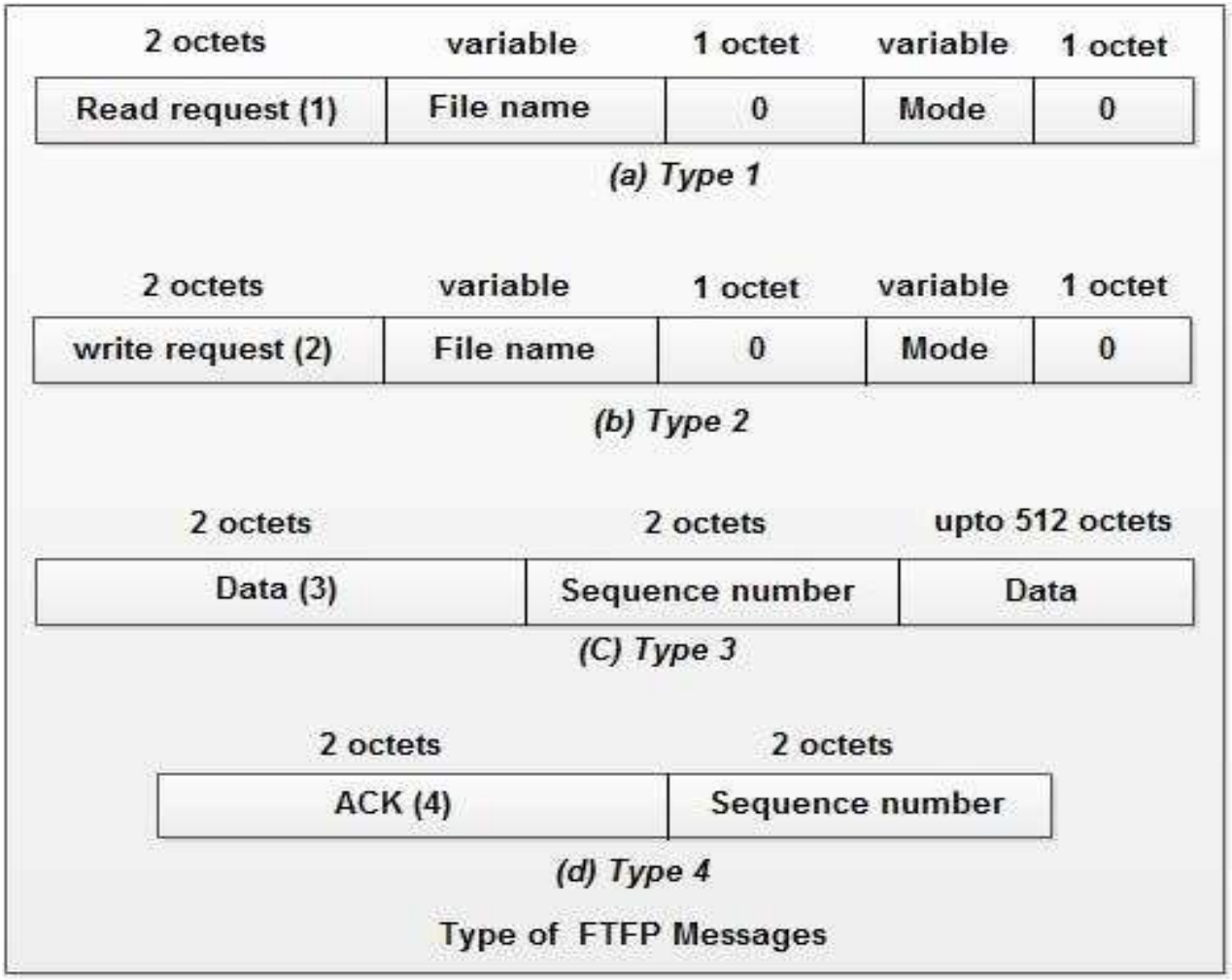
1. **Read request (Type 1).** This is used by the client to get a copy of a file from the server.

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.

# Trivial File Transfer Protocol(TFTP)



# Trivial File Transfer Protocol(TFTP)

**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.

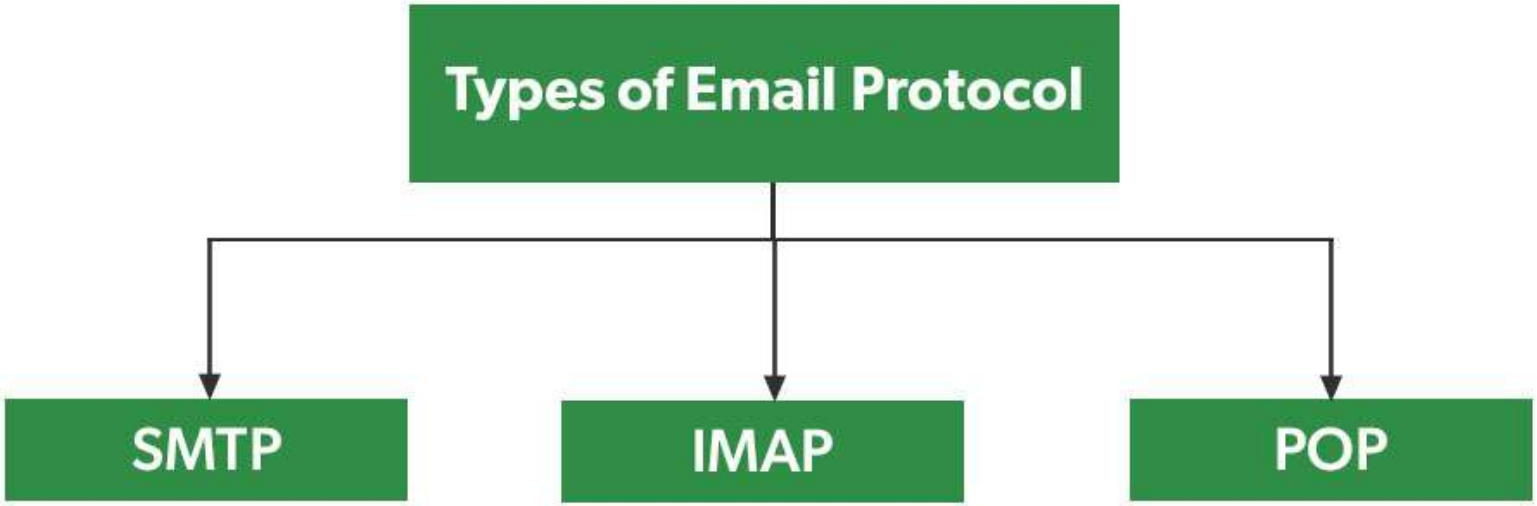
# Email Protocols

- Email protocol is a set of rules defined to ensure that emails can be exchanged between various servers and email clients in a standard manner. This ensures that the email is universal and works for all users.

Three basic types of email protocols involved for sending and receiving mails are:

- SMTP
- POP3
- IMAP

# Email Protocols

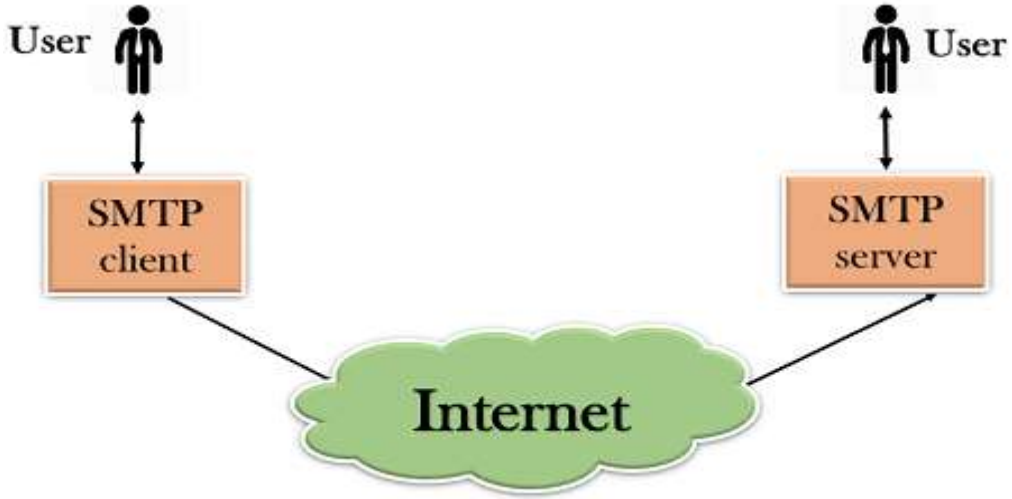


# Simple Mail Transfer Protocol(SMTP)

- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

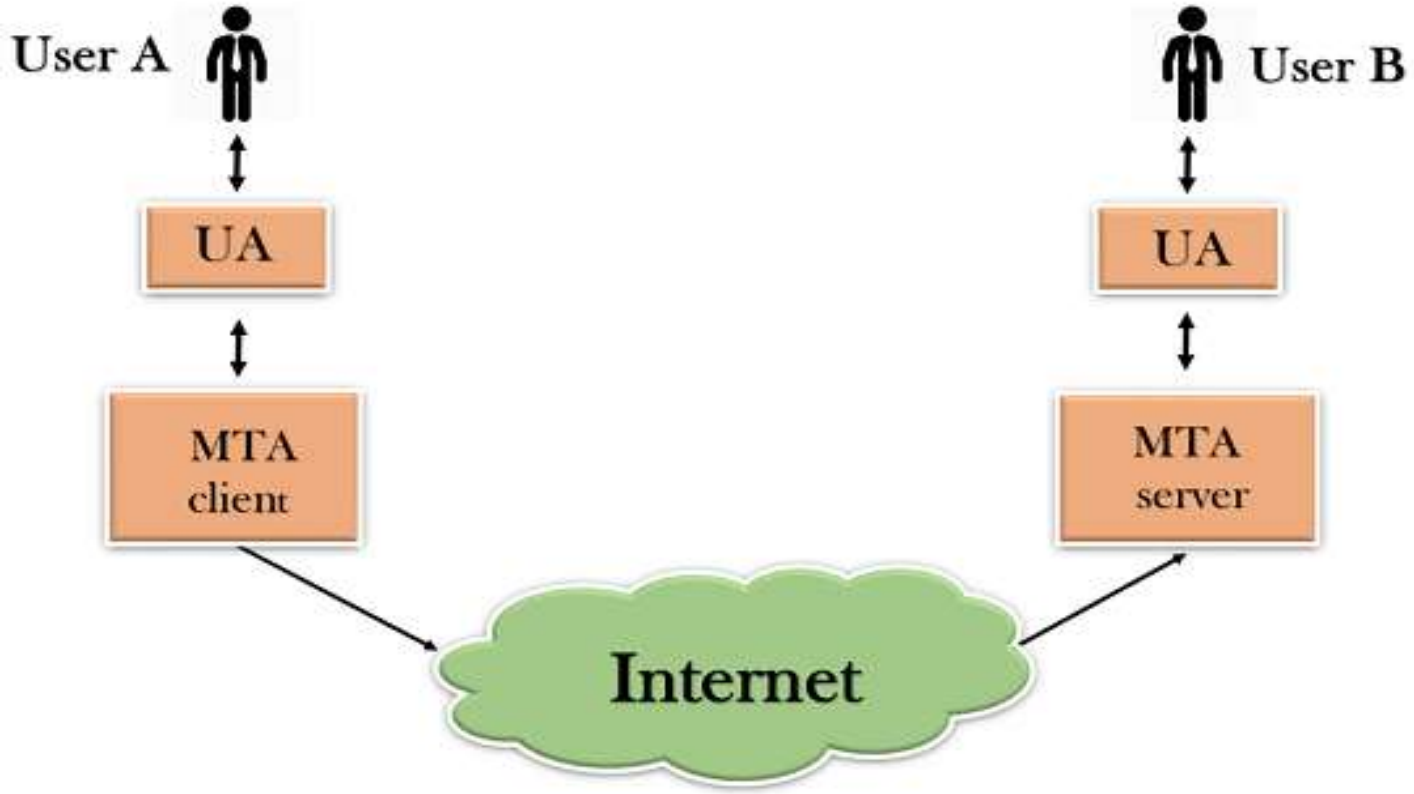
# Simple Mail Transfer Protocol(SMTP)

**Components of SMTP:**



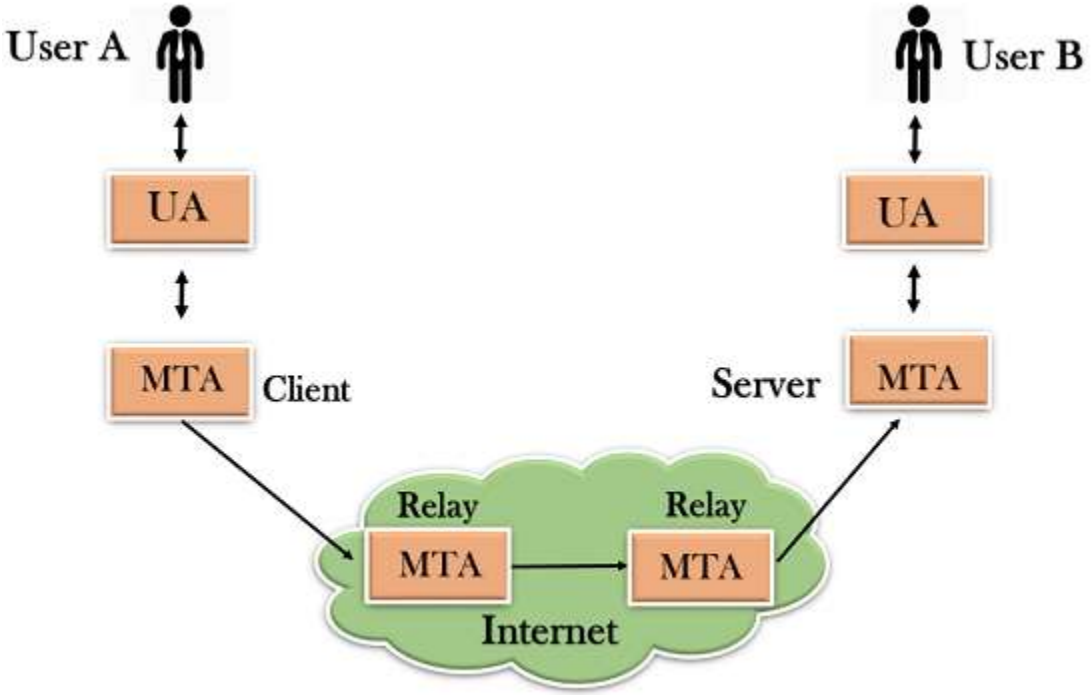

- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

# Simple Mail Transfer Protocol(SMTP)



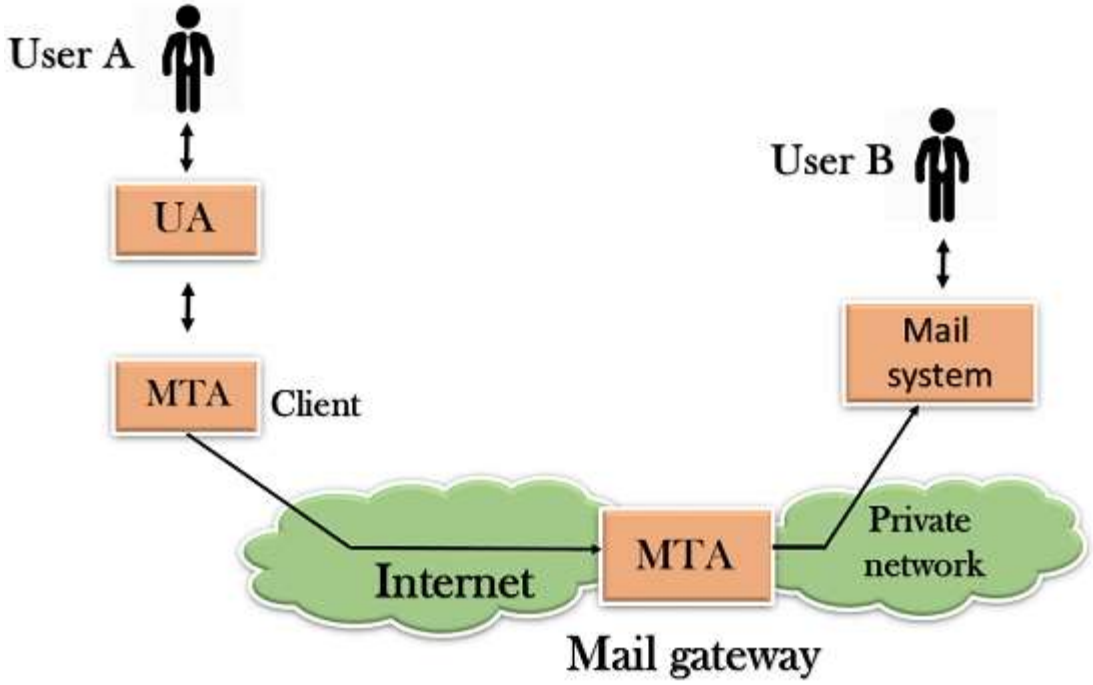
# Simple Mail Transfer Protocol(SMTP)

- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



# Simple Mail Transfer Protocol(SMTP)

- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.



# Simple Mail Transfer Protocol(SMTP)

## Working of SMTP:

### Composition of Mail:

A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.

**Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.

# Simple Mail Transfer Protocol(SMTP)

**Delivery of Mail:**

E-mail addresses contain two parts: username of the recipient and domain name. For example, abc@gmail.com, where “abc" is the username of the recipient and "gmail.com“ is the domain name.

**Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.

**Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

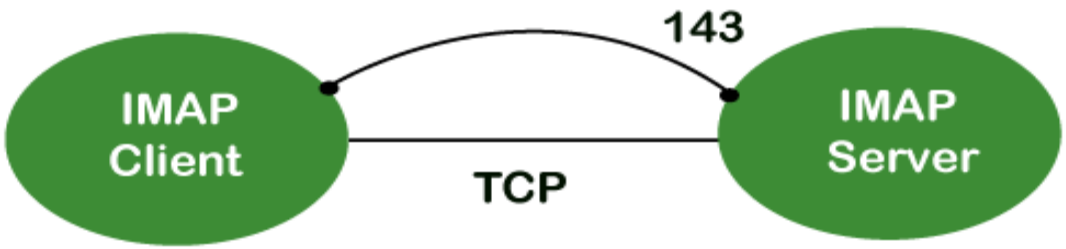
# Internet Message Access Protocol(IMAP)

- It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

- It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.

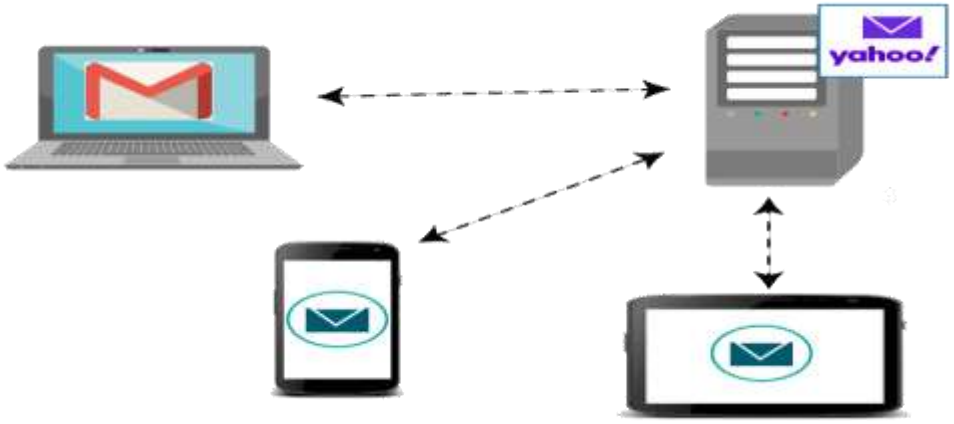
- The IMAP protocol resides on the TCP/IP transport layer which means that it implicitly uses the reliability of the protocol. Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.

# Internet Message Access Protocol(IMAP)




**Port 143:** It is a non-encrypted IMAP port.
**Port 993:** This port is used when IMAP client wants to connect through IMAP securely.

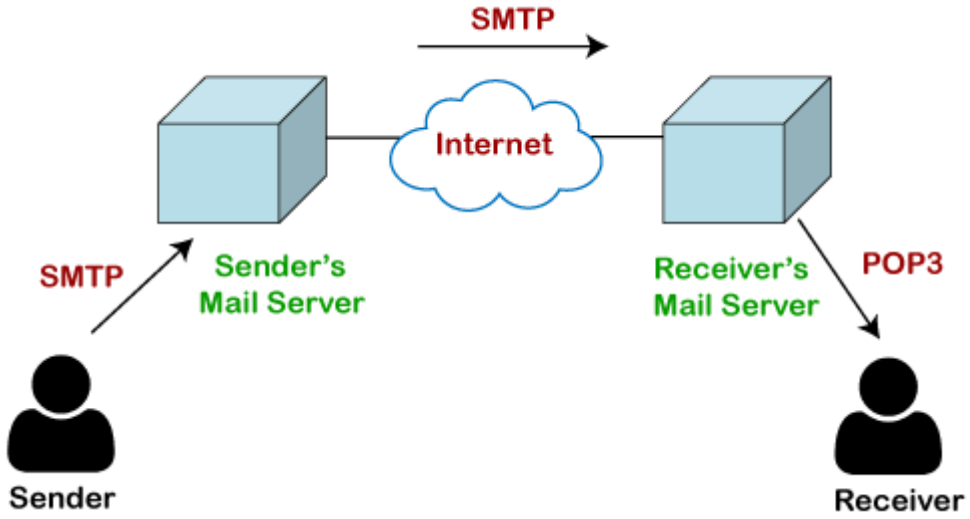
# Internet Message Access Protocol(IMAP)




- The IMAP protocol synchronizes all the devices with the main server. Let's suppose we have three devices desktop, mobile, and laptop as shown in the above figure.
- If all these devices are accessing the same mailbox, then it will be synchronized with all the devices. Here, synchronization means that when mail is opened by one device, then it will be marked as opened in all the other devices, if we delete the mail, then the mail will also be deleted from all the other devices.
- So, we have synchronization between all the devices. In IMAP, we can see all the folders like spam, inbox, sent, etc. We can also create our own folder known as a custom folder that will be visible in all the other devices.

# Post Office Protocol(POP)

- As we know that SMTP is used as a message transfer agent. When the message is sent, then SMTP is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.




- SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

# Simple Network Management Protocol(SNMP)

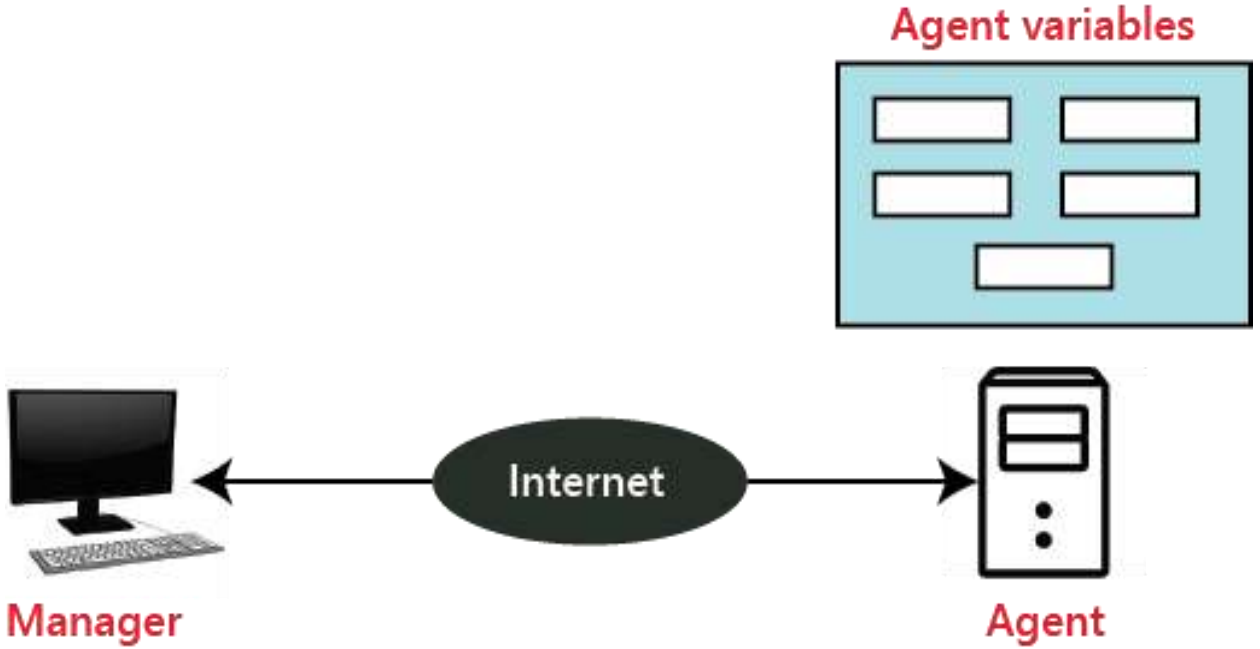
- SNMP was defined by **IETF (Internet Engineering Task Force)**. It is used to manage the network. It is an internet standard protocol that monitors devices in IP networks and collects and organizes the information (data) of these devices.

- SNMP is supported by most network devices such as the hub, switch, router, bridge, server, modem, and printer, etc.

- The concept of SNMP is based on the manager and agent. A manager is like a host that controls a group of agents, such as routers.

- The SNMP sends instructions and messages using both port 161 and port 162. The SNMP agent uses the port 161, and the SNMP manager uses the port 162.

# Simple Network Management Protocol(SNMP)




**SNMP Manager:** It is a computer system that monitors network traffic by the SNMP agent, and it queries these agents, takes answers, and controls them.

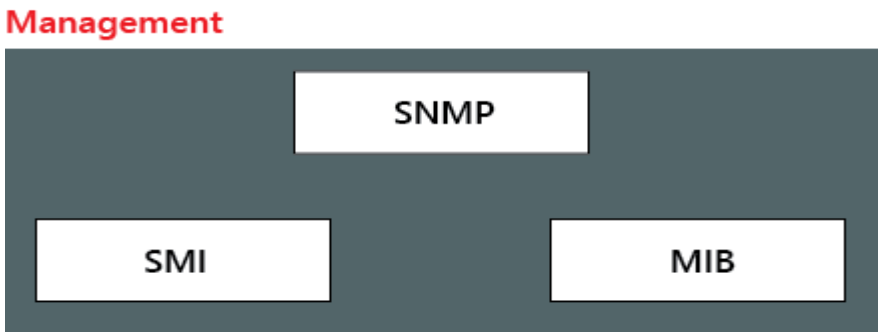
**SNMP Agent:** It is a software program that is located in a network element. It collects real-time information from the device and passes this information to the SNMP manager.

# Simple Network Management Protocol(SNMP)

## Management components:

It has two components

- SMI
- MIB




**SNMP:** It defines the structure of packets that is shared between a manager and an agent.

**SMI(Structure of Management Information):** SMI is a network management component that defines the standard rules for the naming object and object type (including range and length) and also shows how to encode objects and values.

**MIB (Management Information Base):** MIB is the second component of the network management. It is virtual information storage where management information is stored.

# Simple Network Management Protocol(SNMP)

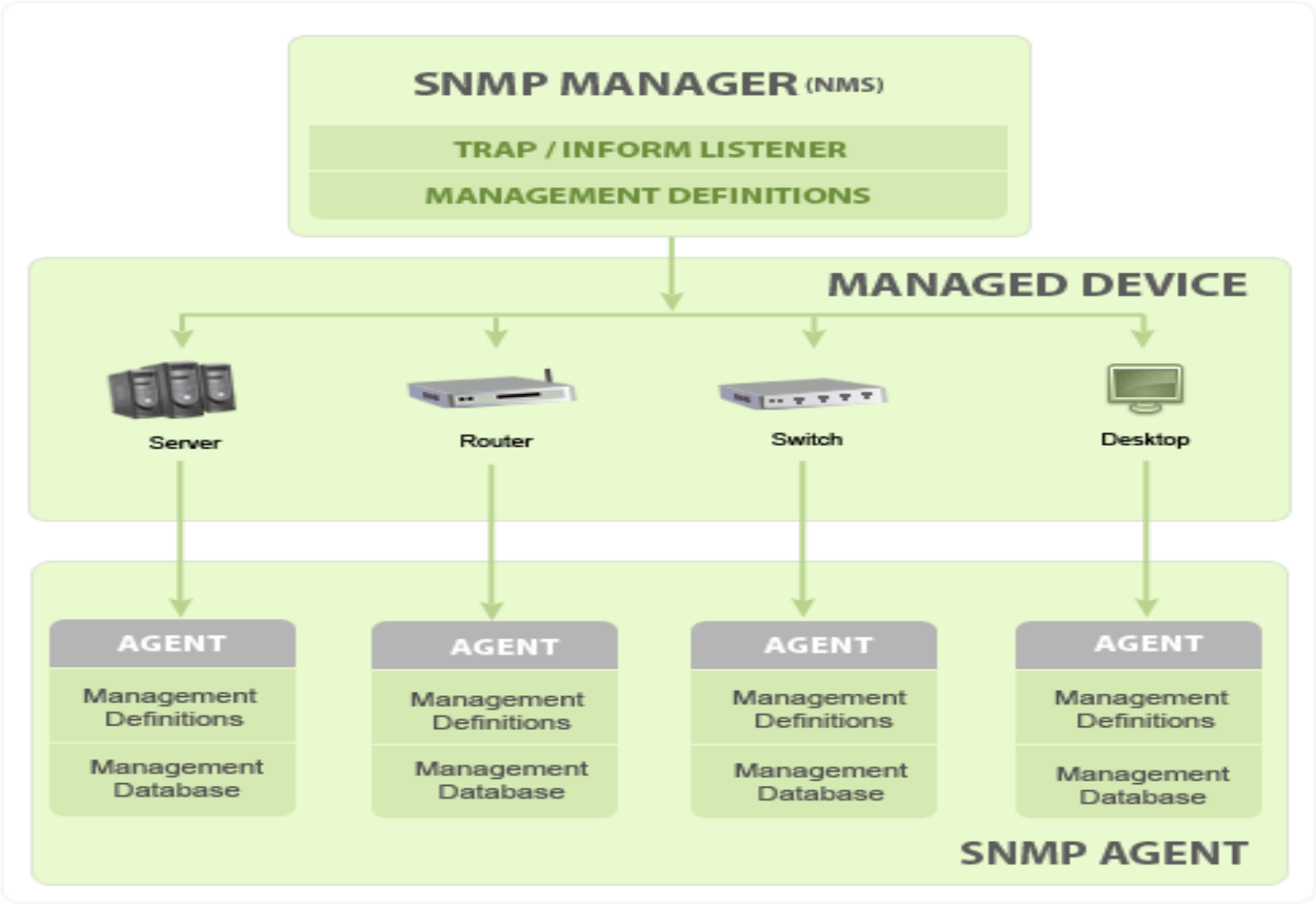
**SNMP Manager's key functions:**

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

**SNMP agent's key functions:**

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non–SNMP manageable network node.

# Simple Network Management Protocol(SNMP)



# Simple Network Management Protocol(SNMP)

**SNMP basic operation:**

**GetRequest:** The GetRequest operation is used by the SNMP manager to derive one or more values from the SNMP agent.

**GetNextRequest:** The GetNextRequest is similar to the GetRequest operation, but it is used to get the next value from the SNMP agent.

**SetRequest:** It is used by the manager to set the value of the agent device.

**Trap:** This command is used by the SNMP agent to send acknowledgment messages to the SNMP manager.

**GetBulkRequest:** It is used by the SNMP manager to retrieve the large data from the SNMP agent.

# Bootstrap Protocol (BOOTP)

- BOOTP (Bootstrap Protocol) is the successor of RARP (Reverse ARP) and the predecessor of DHCP.

- BOOTP uses the UDP transport protocol and rides on top of IP so it can be routed. BOOTP supports relay servers so you can have a central BOOTP server that assigns IP addresses to hosts in all of your subnets.

- Another issue with RARP is that it **only** allows you to assign an IP address, that's it. No default gateway, DNS servers, etc. BOOTP supports all of this. You can assign an IP address, default gateway, subnet mask, DNS servers, and other options.

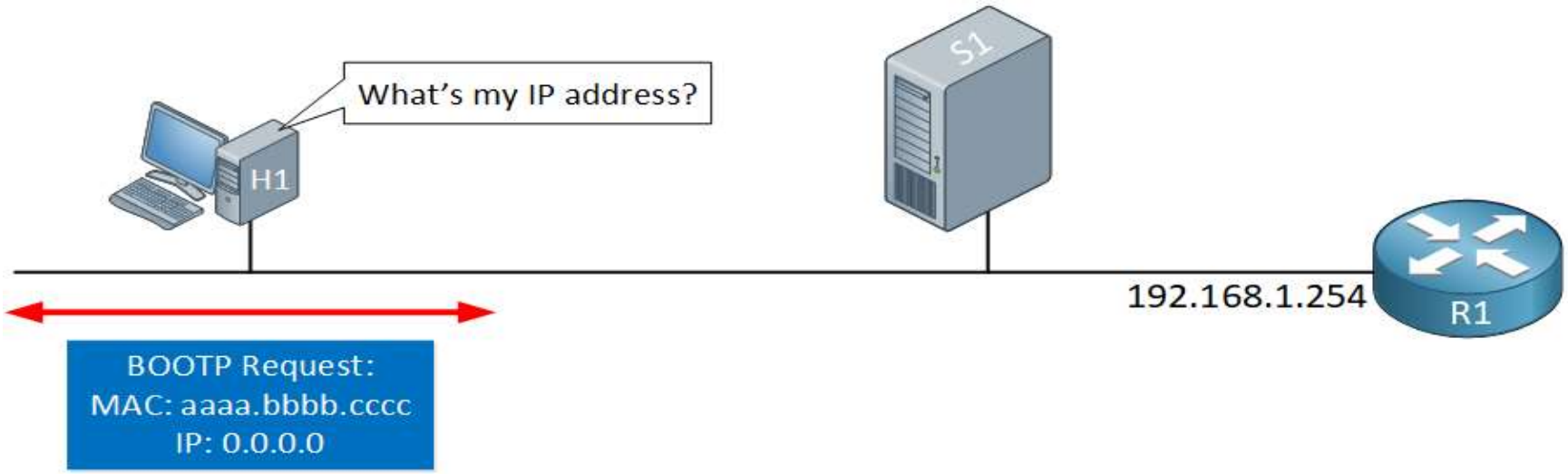
# Bootstrap Protocol (BOOTP)

- BOOTP uses UDP port 67 and 68.

- **BOOTP uses a static database**. When a BOOTP server receives a request, it looks in its database for a matching entry and then returns the result to the host.

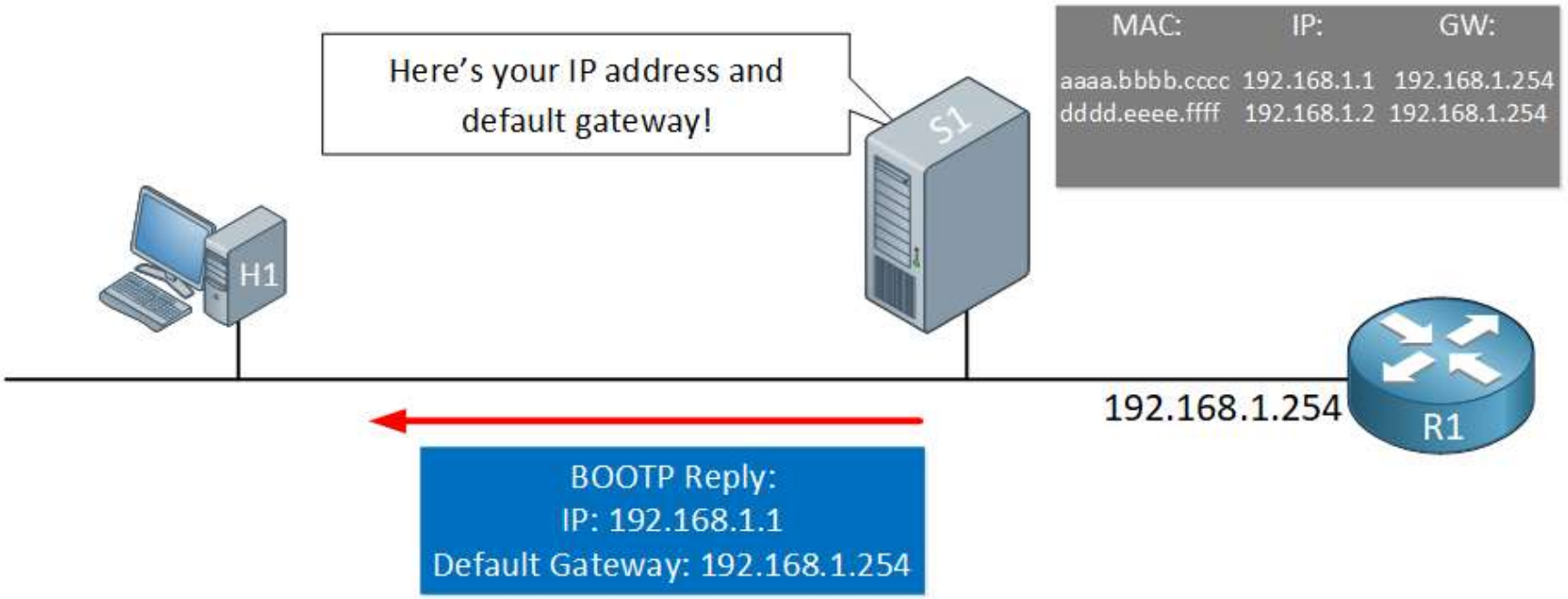
- Here's what the BOOTP process looks like:

# Bootstrap Protocol (BOOTP)




The host sends a BOOTP request and uses UDP source port 68 and destination port 67. This packet is a broadcast so everything in the broadcast domain receives it. On our network, we have a BOOTP server listening on UDP port 67.

# Bootstrap Protocol (BOOTP)




The server sees the broadcast packet from the host and since it's listening on UDP port 67, it processes the packet. The server then looks in its database to find a matching entry for the MAC address of the host. When there is a match, it returns the information to the host with a unicast packet.