Syllabus

★ **The Application Layer:**

- Domain name system

- Electronic mail

- World Wide Web: architectural overview

- Dynamic web document

★ **Application Layer Protocols**

- Http Protocol

- Simple Mail Transfer Protocol

- Simple Network Management Protocol

- File Transfer Protocol

- Telnet

Domain Name System(DNS)
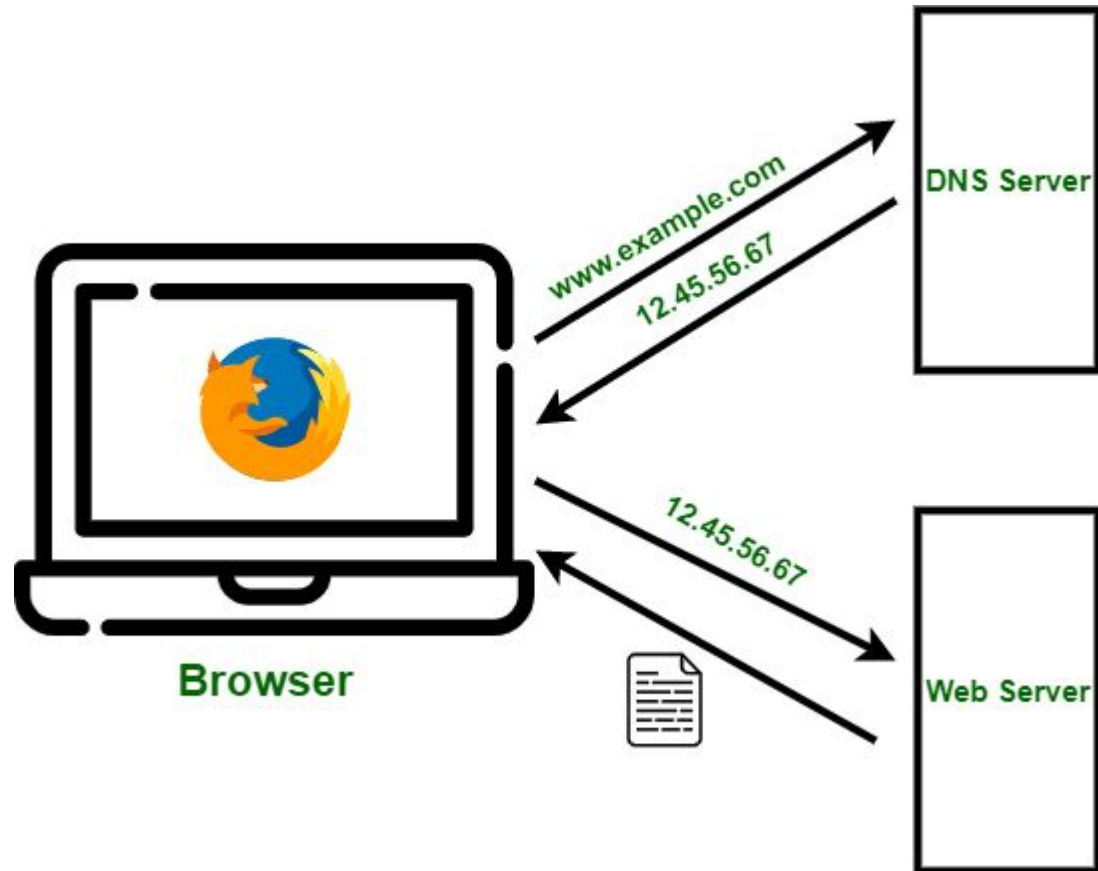
- The DNS Name Space

- Name Servers

★ DNS is an abbreviation of Domain Name System (or) Domain Name Service. It is an application layer protocol.

★ Translates internet **domain names to their unique IP addresses.**

Host Name → Domain Name Service (DNS) → IP Address

What is the Need of DNS?

★ Every host is identified by the IP address but remembering numbers is very difficult for people.

★ So DNS is used to convert the domain name of the websites to their numerical IP address.

Working of Domain Name System (DNS) Server

DNS Resolver?

- To map a host_name onto an IP address, an application program calls **a library procedure** called **the resolver**, passing it the name as a parameter.
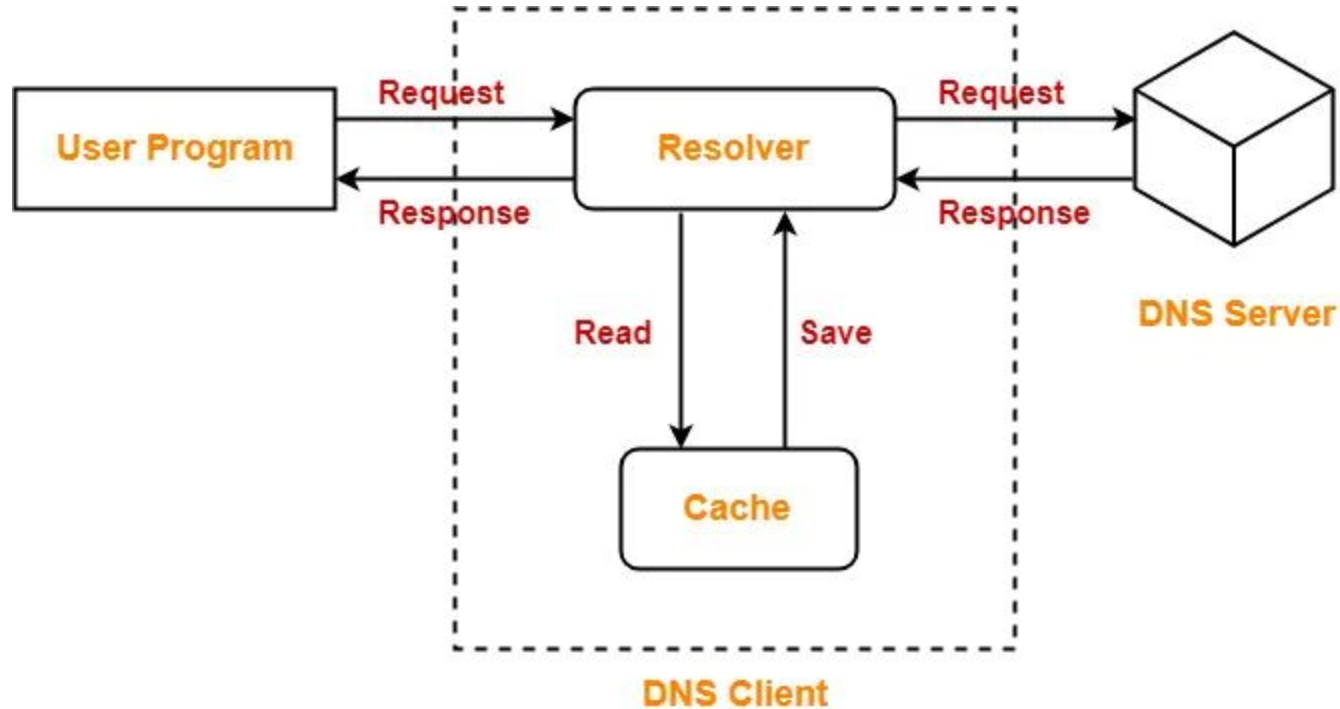
The DNS Name Space

- Managing a large and constantly changing set of names is a nontrivial problem.

- In the postal system, name management is done by requiring letters to specify the country, state, city, street address, and name of the addressee.DNS works the same way.

- For the Internet, the top of the **naming hierarchy** is managed by an organization called **ICANN (Internet Corporation for Assigned Names and Numbers).**

- Conceptually, the Internet is divided into over **250 top-level domains**, where each domain covers many hosts.

- **Each domain** is partitioned into **subdomains**, and these are further partitioned, and so on.

- All these domains can be represented by a tree, as shown in Fig. 7-1.

- The **leaves** of the tree represent domains that have no subdomains

- A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.
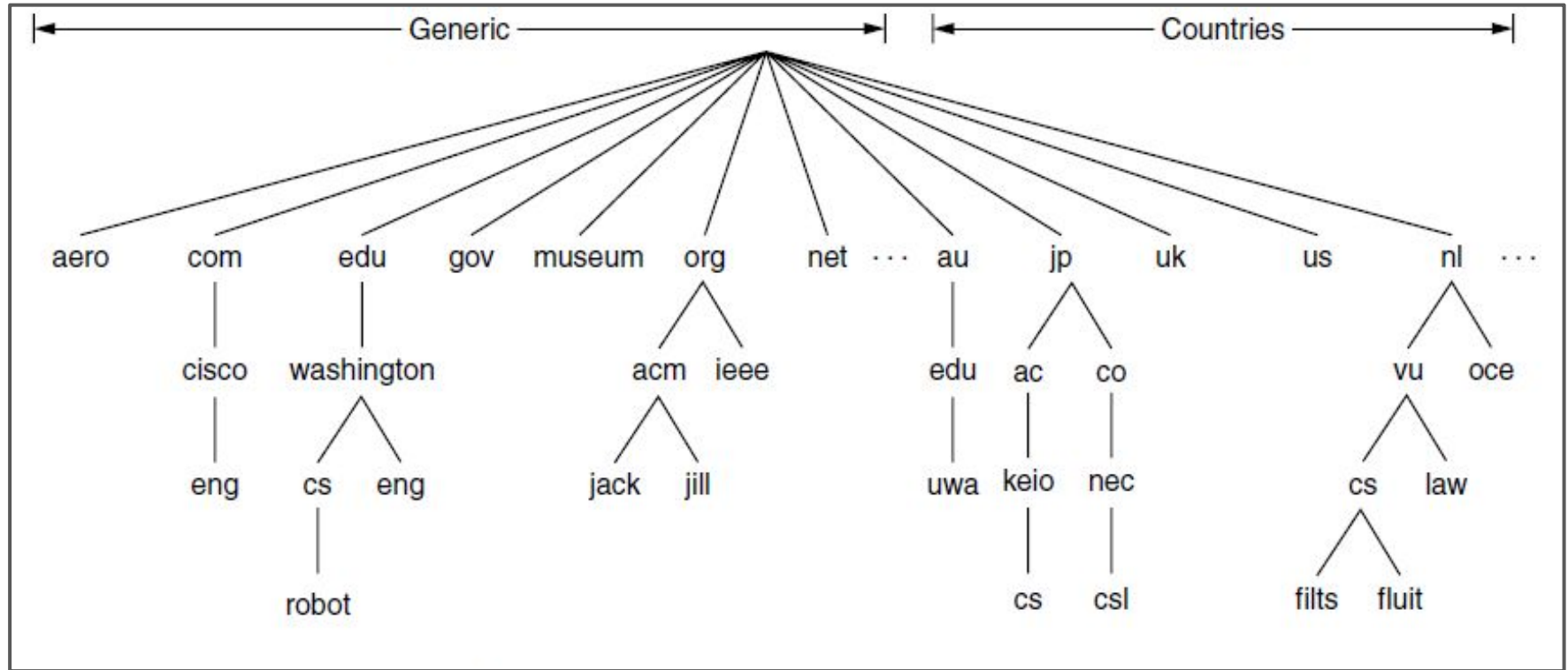
The Internet Domain Name Space

Figure 7-1

The DNS Name Space

- The name of a host is divided into various pieces called **domains**. These domains are structured in a hierarchical structure so that top-level domains are listed at the top of the hierarchy and low levels are listed at the bottom.

- When **searching for a host**, we start our searching in **ascending order, i.e., from leaf nodes to root nodes.**

Types of Domain:

1. **Generic domains**

2. **Country domain**

- **Generic domains:**
  - .com(commercial),
  - .edu(educational),
  - .mil(military),
  - .org(nonprofit organization),
  - .net(similar to commercial) all these are generic domains.
- **Country domain:**
  - .au (Australia)
  - .in (India)
  - .us (United States)
  - .uk (United Kingdom)
 - .nl (Netherlands)
  - .jp (Japan)

Domain Name and labels

- Each node of the tree has **a domain name.**

- A Full domain name is basically a sequence of labels that are usually **separated by dots(.)**

- The domain name is **always read from the leaf node to the root node.**

- The last label is the label of the root that is always null.

- All this means that the full domain name always ends in the null label, which means that the last character is always a dot because the null string is nothing.
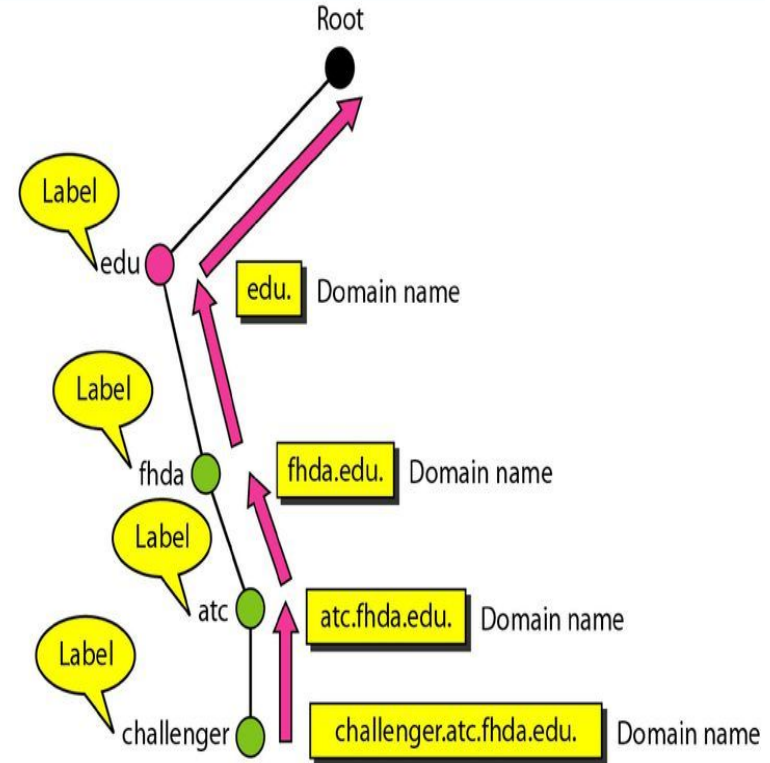
Name Servers

Example of a resolver looking up a remote name in 9 steps
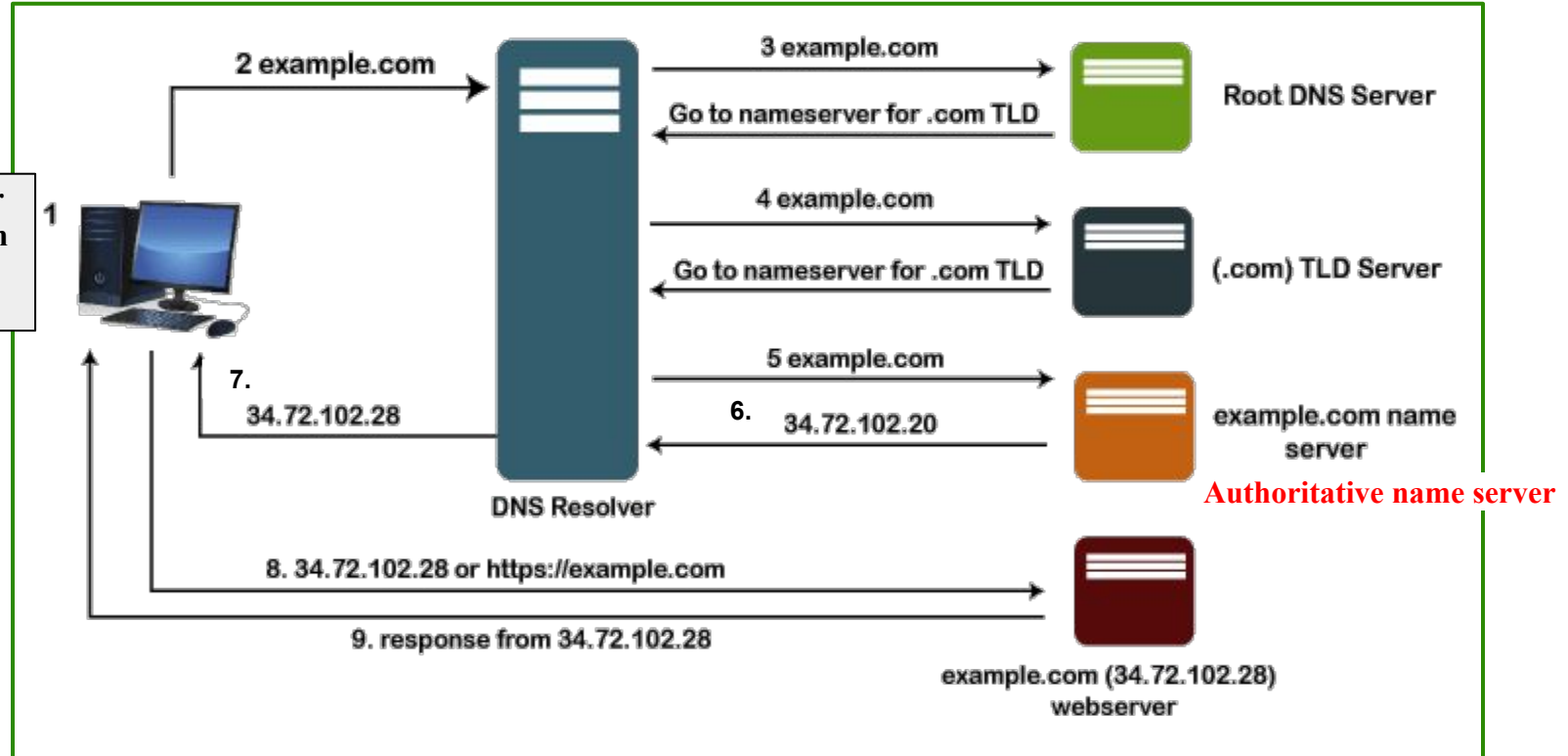
1. Users open a web browser, **enter example.com** in the address bar, and presses Enter button.

2. The request, for example.com is routed to a DNS resolver, which manages by the user's Internet service provider.

3. The **DNS resolver** forwards the request, for example.com to **a root DNS server.**

4. The DNS resolver again forwards the request, for example.com, this time to one of the **TLD(Top Level Domain)name servers for .com domains**. The name server for .com domains responds to the request with the 2 or 4 name servers associated with the example.com domain.

5. The DNS resolver chooses an example.com, **the authoritative name server**, and forwards the request for example.com to that name server.

6. The website's name server looks in the example.com hosted zone for the example.com a record, to get the associated value, such as the IP address for a web server, 34.72.102.28, and returns the IP address to the DNS resolver.

7. Finally, The DNS resolver for the ISP has the IP address that the user needs. The resolver returns that value to the web browser. The DNS resolver can store the IP address, for example.com.

8. The web browser sends a request, for example.com using the IP address that it got from the DNS resolver. This is where the actual content is.

9. The web server or other resource at 34.72.102.28 returns the web page, for example.com to the web browser, and the web browser displays the page.

Electronic mail(e-mail)

★ Electronic mail, or more commonly email, is a method of **exchanging messages** over the internet.

★ Electronic mail allows a message to **include text, audio, and video**. It also allows one message to be sent to one or more recipients.

★ Faster and cheaper than paper mail, email has been a popular application since the early days of the Internet.

★ **E-mail systems support 5 basic functions:-**

  ○ Composition

  ○ Transfer

  ○ Reporting

  ○ Displaying

  ○ Disposition

(a) Composition:

- It refers to the process of creating messages and answers. Any text editor is used for body of the message.

- While the system itself can provide assistance with addressing and numerous header fields attached to each message.
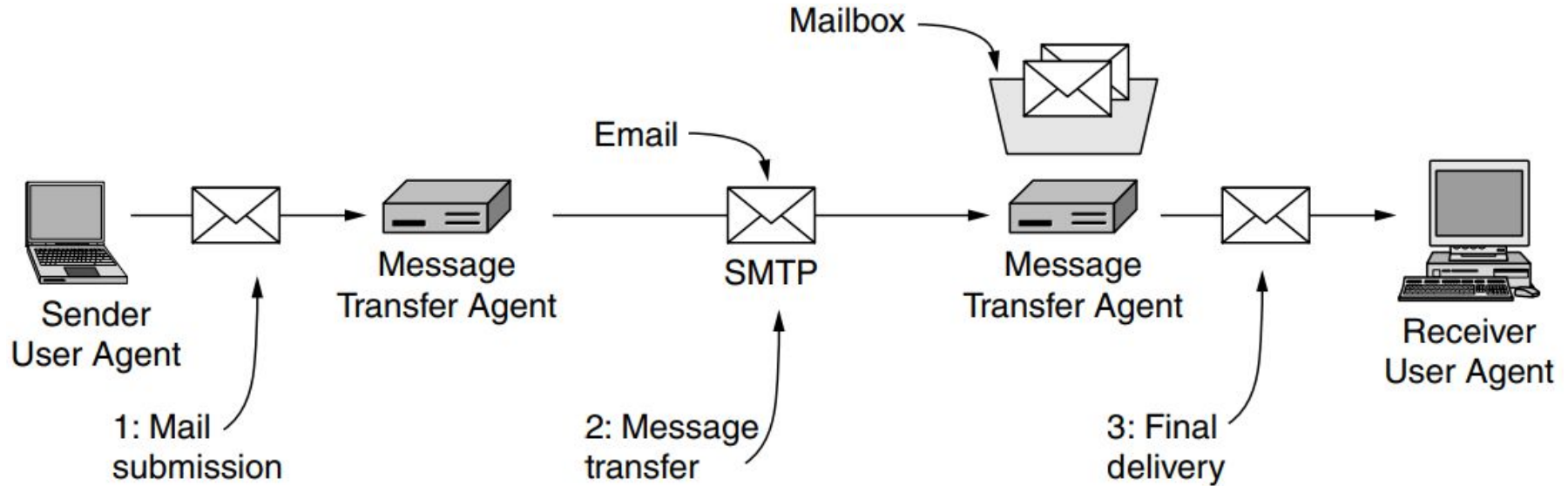
(b) Reporting:

- It has to do with telling the originator what happened to the message that is, whether it was delivered, rejected (or) lost.

(c) Transfer: It refers to moving messages from originator to the recipient.

(d) Displaying: Incoming messages are to be displayed so that people can read their email.

(e) Disposition: It concerns what the recipient dose with the message after receiving it.

Architecture of the email system

Mailbox

Email

SMTP

Sender
User Agent

Message
Transfer Agent

Message
Transfer Agent

Receiver
User Agent

1: Mail
submission

2: Message
transfer

3: Final
delivery

Architecture of the email system :-

- The architecture of the email system is shown in Fig. 7-7.

- It consists of two kinds of subsystems:

  - **The UserAgent :** which allow people to read and send email

  - **The Message Transfer Agents** : which move the messages from the source to the destination. We will also refer to message transfer agents informally as **mail servers**.

User Agent:

➔ The user agent is a program that provides **a graphical interface, or sometimes a text- and command-based interface** that lets users interact with the email system.

➔ It includes a means to compose messages and replies to messages, display incoming messages, and organize messages by filing, searching, and discarding them.

➔ The act of sending new messages into the mail system for delivery is called mail submission.

Message Transfer Agent:

➔ The message transfer agents are typically system processes. They run in the background on mail server machines and are intended to be always available.

➔ Their job is to **automatically move email through the system from the originator to the recipient with SMTP** . This is the message transfer step.

SMTP (Simple Mail Transfer Protocol):

➔ It is a set of rules and conventions used to transmit email messages between servers.

➔ SMTP is an essential component of email communication and **is responsible for routing and delivering outgoing email messages from the sender's email client or server to the recipient's email server.**

➔ **It reports back the delivery status and any errors.**

Message Format of an email :

➔ Email messages follow a specific format that includes various components to ensure proper communication and presentation. Here's an overview of the key message formats in an email system.
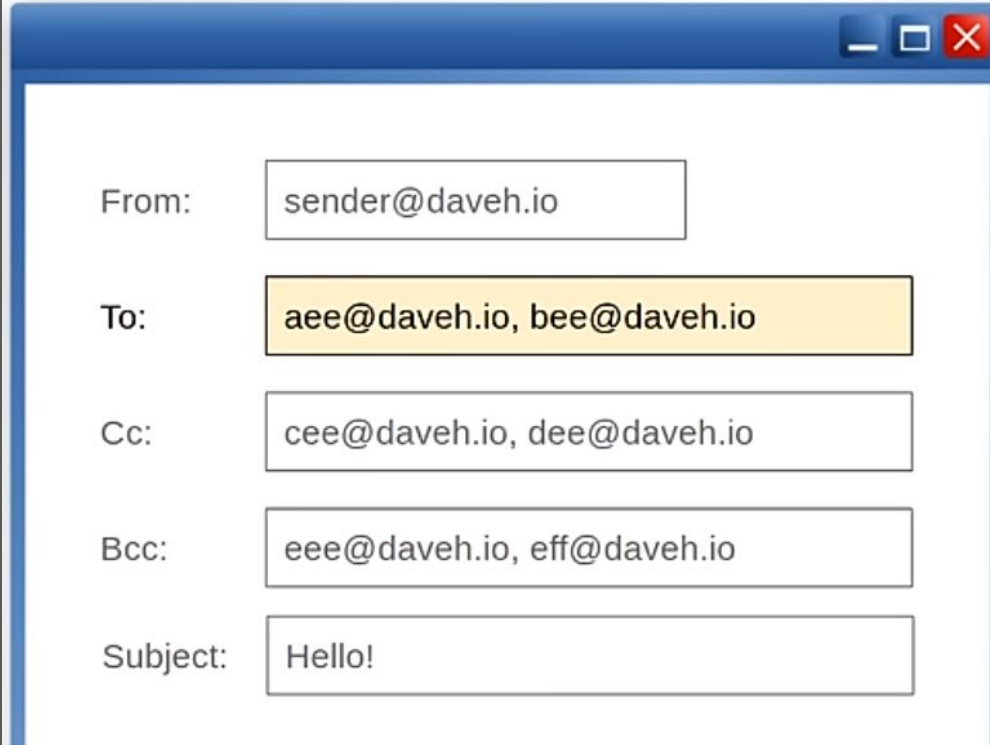
1. **Header Field:**

Header	Meaning
To:	Email address(es) of primary recipient(s)
Cc:	Email address(es) of secondary recipient(s)
Bcc:	Email address(es) for blind carbon copies
From:	Person or people who created the message

CC (Carbon Copy):

- When you CC someone on an email, all recipients can see who else received the email.
- It's commonly used when you want to keep others informed about the email conversation but they are not directly involved in it.

BCC (Blind Carbon Copy):

- When you BCC someone on an email, the recipients in the "To" and "CC" fields can't see that person's email address.
- It's used when you want to include someone in the conversation without letting other recipients know.

From:	sender@daveh.io
To:	aee@daveh.io, bee@daveh.io
Cc:	cee@daveh.io, dee@daveh.io
Bcc:	eee@daveh.io, eff@daveh.io
Subject:	Hello!

CC (Carbon Copy) and BCC (Blind Carbon Copy) are both used in email to include additional recipients beyond the primary recipient.

2. Message Body:

Text Content: This is the main part of the message where the sender writes the actual text. It can include plain text or formatted text (HTML).

3. Multipurpose Internet Mail Extensions (MIME):

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of **audio, video, images, and application programs.**

SMTP(Simple Mail Transfer Protocol)

★ **SMTP (Simple Mail Transfer Protocol)** is an application layer used in sending and receiving email.

★ SMTP is used most commonly by email clients, including Gmail, Outlook, Apple Mail and Yahoo Mail.

SMTP Fundamentals

★ The client who wants to send the mail opens **a TCP connection** to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through **port 25**. After successfully establishing a TCP connection the client process sends the mail instantly.

★ **If a message cannot be delivered**, an error report containing the first part of the undeliverable message is returned to the sender.

SMTP Model
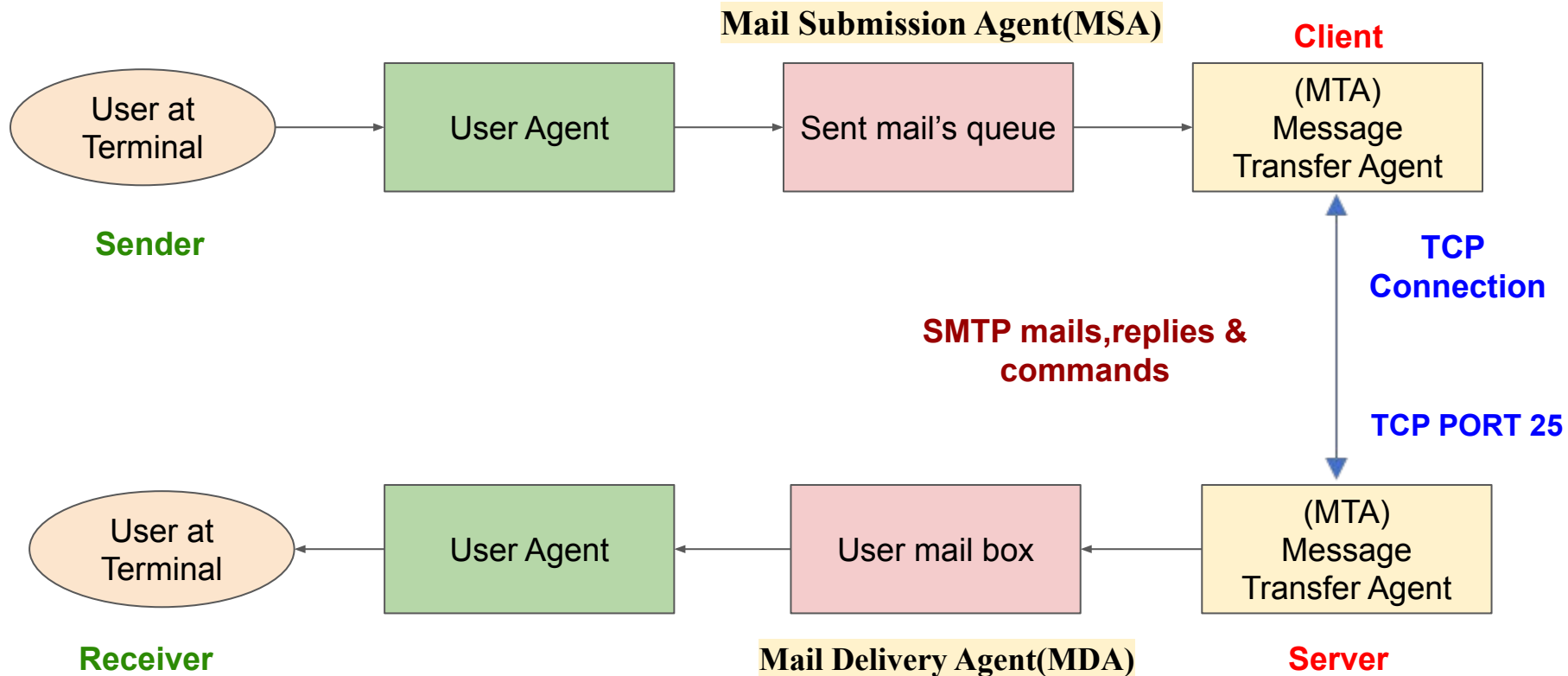
Components of SMTP

1. **User Agent (MUA)**

2. **Mail Submission Agent (MSA)**

3. **Mail Transfer Agent (MTA)**

4. **Mail Delivery Agent (MDA)**

1. Mail User Agent (MUA):

★ It is a computer application that helps you in **sending and retrieving mail**.

★ It is responsible for creating email messages for transfer to the mail transfer agent(MTA).

2. Mail Submission Agent (MSA):

- It is a computer program that basically receives mail from User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.

3. Mail Transfer Agent(MTA):

★ It is basically software that has the work to transfer mail from one system to another with the help of **SMTP**.

4. Mail Delivery Agent(MDA):

- A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.

Some SMTP Commands

1. **HELO/EHLO**

- The HELO command initiates the SMTP session conversation.

- The client greets the server and introduces itself. As a rule, HELO is attributed with an argument that specifies the domain name or IP address of the SMTP client.

2. **MAIL FROM**

- The MAIL FROM command initiates a mail transfer.

3. **RCPT TO**

- The RCPT TO command specifies the recipient.

4. **DATA**

- With the DATA command, the client asks the server for permission to transfer the mail data.

POP3 & IMAP Protocols

POP3 & IMAP Protocols

1. **POP3** (**Post Office Protocol, version 3**)

- POP3 is a simple and older **email retrieval protocol**.

- It is primarily designed for **downloading email messages to a local device (e.g., a computer or a mobile device).**

- POP3 operates over non-secure **port 110**

- POP3 doesn't support advanced mailbox management features like organizing emails into folders on the server.

2. **IMAP** (**The Internet Message Access Protocol**)

- IMAP is a **much more advanced email retrieval protocol** compared to POP3.

- It allows users to access and manage their email messages stored on mail server.

- The IMAP operates on **port 143**.

World Wide Web: Architectural overview

" *World Wide Web*, which is also known as *a Web*, is **a collection of websites or web pages stored in web servers** and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. "

- **Tim Berners-Lee**, a British scientist, invented the World Wide Web (WWW) in 1989, while working at CERN.

- The Web was originally conceived and developed to meet the demand for automated information-sharing between scientists in universities and institutes around the world.

- CERN, where Tim Berners worked, is a community of more than 1700 scientists from more than 100 countries.

- So there was a need for reliable communication tools so that they can exchange information.

Tim Berners-Lee

Architectural Overview

Web page:

- The **Web** consists of a vast, worldwide collection of content in the form of **Web pages**, often just called **pages** for short. Each

Hypertext:

- In the context of the web, hypertext is text that contains links (hyperlinks) to other web pages. These links are usually displayed as underlined or differently colored text and are clickable.
- The idea of having one page point to another, now called **hypertext**.

Web browser:

- Pages are generally viewed with a program called **a browser**. Firefox, Internet Explorer, and Chrome are examples of popular browsers.
- The browser fetches the page requested, interprets the content, and displays the page, properly formatted, on the screen.
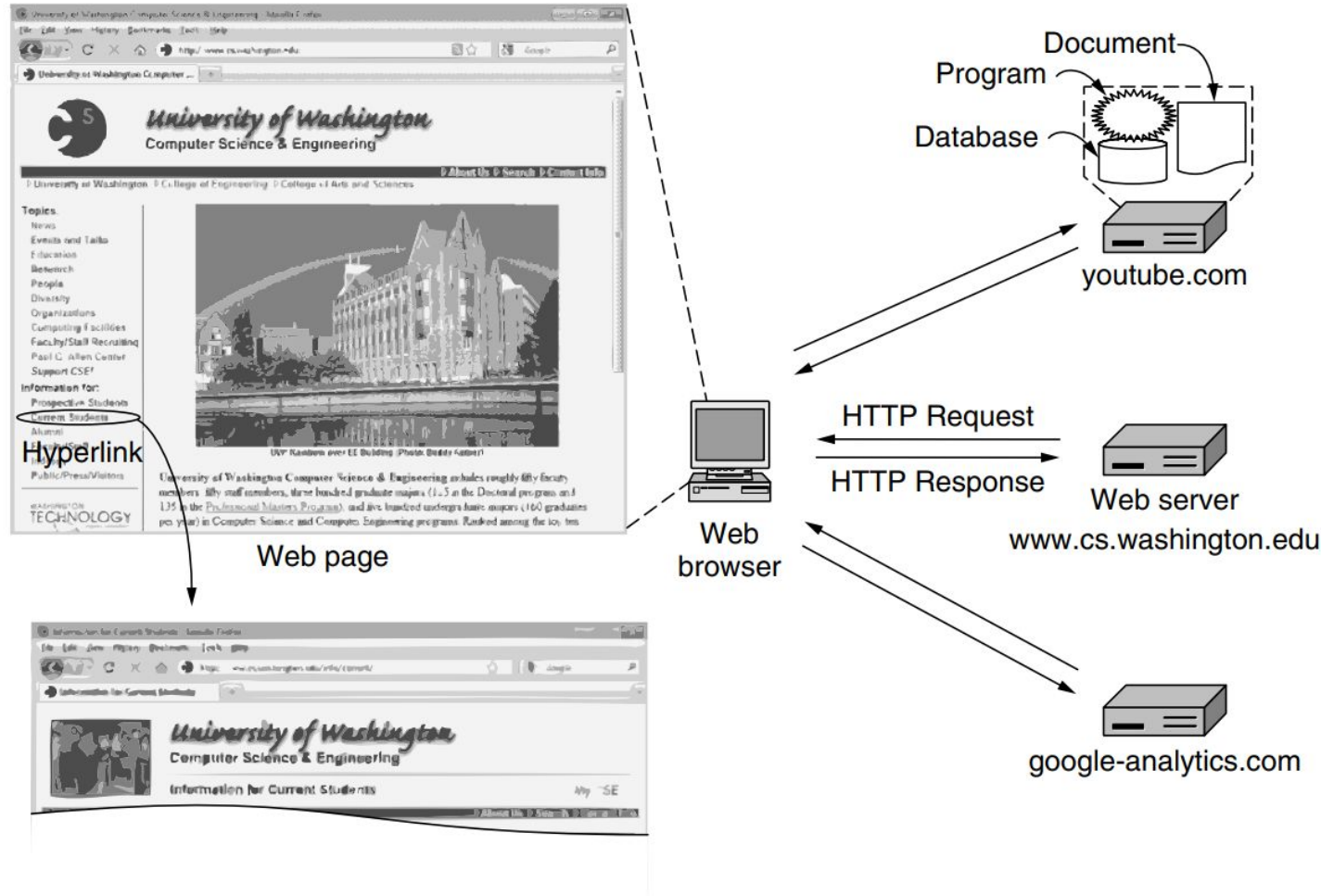
Figure 7-18. Architecture of the Web.

- The basic model behind the display of pages is also shown in Fig. 7-18.

- The browser is displaying a Web page on the client machine.

- Each page is fetched by sending a request to one or more servers, which respond with the contents of the page.

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

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

- **URLs have three parts:** (Eg: **http://www.cs.washington.edu/index.html**)

  a. The protocol (**http**),

  b. The DNS name of the machine on which the page is located, (**www.cs.washington.edu**)

  c. The path uniquely indicating the specific page (**index.html**)

As an example, the URL of the page shown in Fig. 7-18 is http://www.cs.washington.edu/index.html)

Client Side:

1. The browser determines the **URL** (by seeing what was selected).

2. The browser asks DNS for the IP address of the server **www.cs.washington.edu.**

3. DNS replies with **128.208.3.88.**

4. The browser makes **a TCP connection to 128.208.3.88 on port 80**, the well-known **port** for the **HTTP protocol.**

5. It sends over an **HTTP request** asking for the page **/index.html.**

6. **The www.cs.washington.edu server** sends the page as an HTTP response, for example, by sending the file **/index.html**

7. **The browser displays the page /index.html** as it appears in Fig. 7-18.

8. The **TCP connections are released** if there are no other requests to the same servers for a short period.

The Server Side:

1. **Accept a TCP connection** from a client (a browser).

2. **Get the path** to the page, which is the name of the file requested.

3. **Get the file (from disk).**

4. **Send the contents of the file** to the client.

5. **Release the TCP connection**.

HTTP Protocol(Hypertext Transfer Protocol)

- HTTP (HyperText Transfer Protocol), the protocol that is **used to transport all this information between Web Servers and Clients**.

- HTTP is a simple **request-response protocol** that normally **runs over TCP**.

- It specifies what messages clients may send to servers and what responses they get back in return.
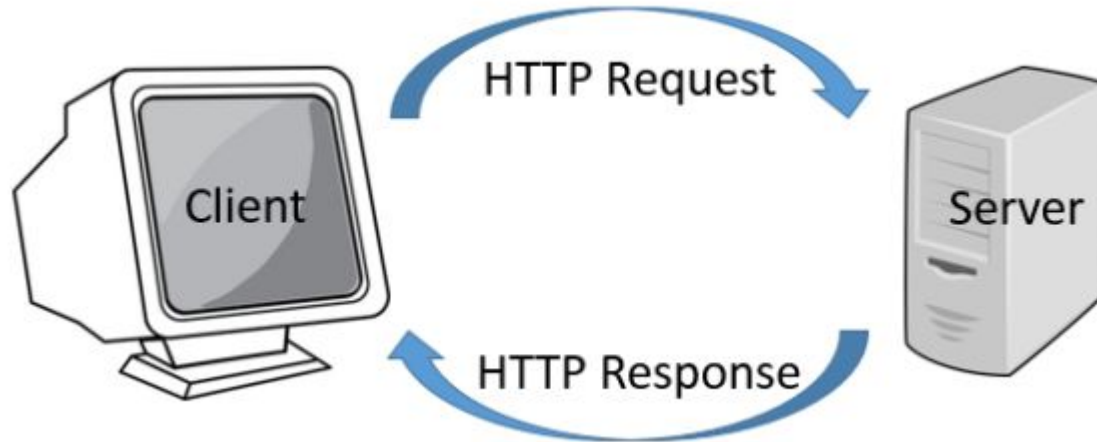
Types of HTTP Connections

1. **Non-Persistent Connection**

2. **Persistent Connection**

3. **Pipelined Connection**

1. Non-Persistent Connection [HTTP/1.0 connection]

➜ Also known as "HTTP/1.0" connection.

➜ In a non-persistent connection, a new TCP connection is established for each HTTP request/response exchange.

➜ In non-persistent connection HTTP, there can be **at most one webpage that can be sent over a single TCP connection**. This means that for each webpage that is to be sent from source to destination, a new connection will be created

➜ After each request-response cycle, the connection is closed.

➜ This approach was **used in early versions of HTTP** and is relatively **inefficient** because it incurs the overhead of establishing and closing a new connection for each resource request, leading to slower page loading times.
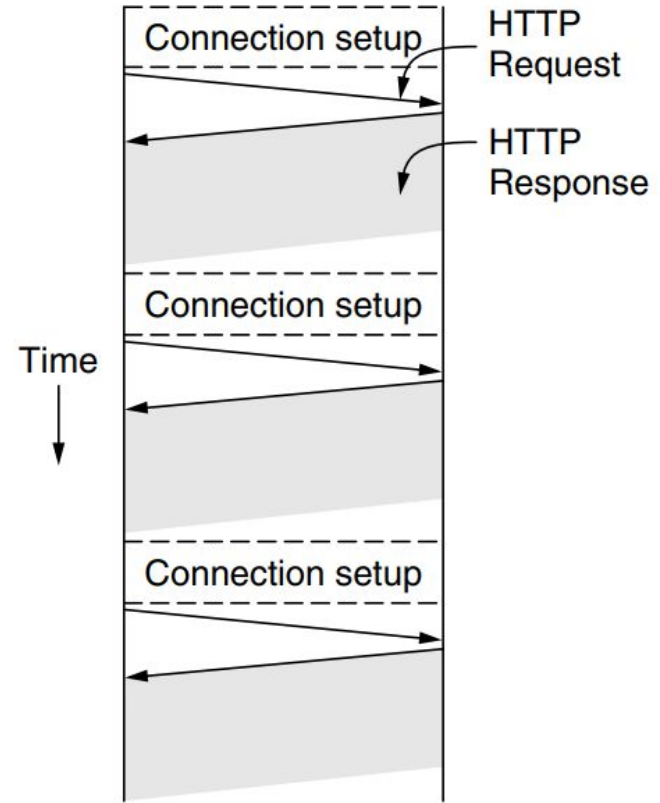
Fig:
Multiple connections and sequential requests.

2. Persistent Connection [HTTP/1.1 connection]

➔ Also known as a "keep-alive" or "HTTP/1.1" connection.

➔ In a persistent connection, the TCP connection between the client and the server remains open after the initial request and response, allowing **multiple HTTP requests and responses** to be sent over **the same connection.**

➔ This means that multiple web pages can be transmitted from source to destination on a single HTTP connection

➔ This reduces the overhead associated with opening and closing connections for each resource, leading to faster loading times and improved performance.

➔ **All modern web browsers like Mozilla Firefox and Google Chrome use persistent HTTP connections**.
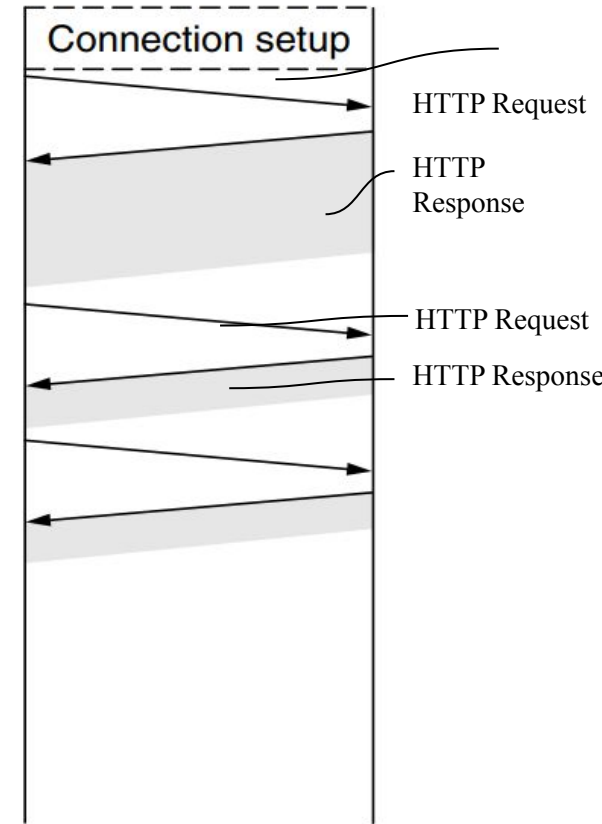

Fig:
A persistent connection and sequential requests

3. Pipelined Connection:

- HTTP pipelining is a feature that allows **multiple HTTP requests** to be sent to the server **without waiting for each response to arrive before sending the next request.**

- With pipelining, the client can send a series of requests in rapid succession without waiting for the responses, which can help reduce latency.

- However, pipelining is not always well-supported by all servers and intermediaries, and careful response handling is required to ensure that responses are processed in the correct order.
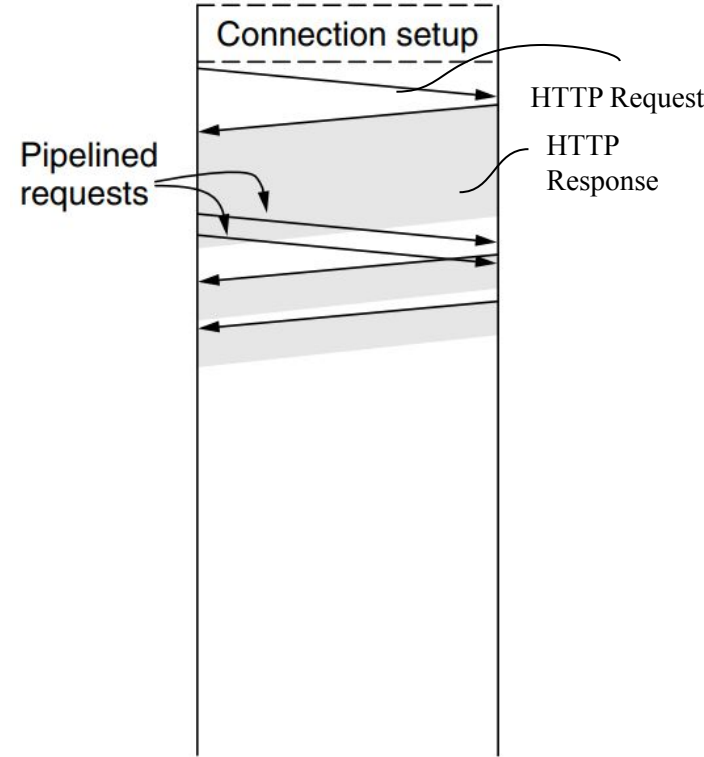

Connection setup

HTTP Request

HTTP Response

Pipelined requests

Fig:
A persistent connection and pipelined request

Simple Network Management Protocol(SNMP)

- **SNMP (Simple Network Management Protocol)** is an application layer protocol that utilizes the UDP protocol to manage routers, hubs, and switches on an IP network.

- Simple Network Management Protocol (SNMP) is a protocol used in **network management systems to monitor and manage network devices and their functions**.

- SNMP is a widely used protocol that is enabled on a wide range of operating systems, including **Windows Server, Linux servers**, and network devices such **as routers and switches.**

- SNMP is an essential part of network management and plays a crucial role in ensuring the reliability and performance of networked systems.

- On a target system, SNMP enumeration is used to list user accounts, passwords, groups, system names, and devices.

Understand SNMP

SNMP consists of 3 items:

1. **SNMP Manager** (sometimes called Network Management System – NMS): a software runs on the device of the network administrator (in most case, a computer) to monitor the network.

2. **SNMP Agent:** a software runs on network devices that we want to monitor (router, switch, server…).

3. **Management Information Base (MIB):** is the collection of managed objects. This components makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP Manager can ask the Agent (and the Agent can understand them).

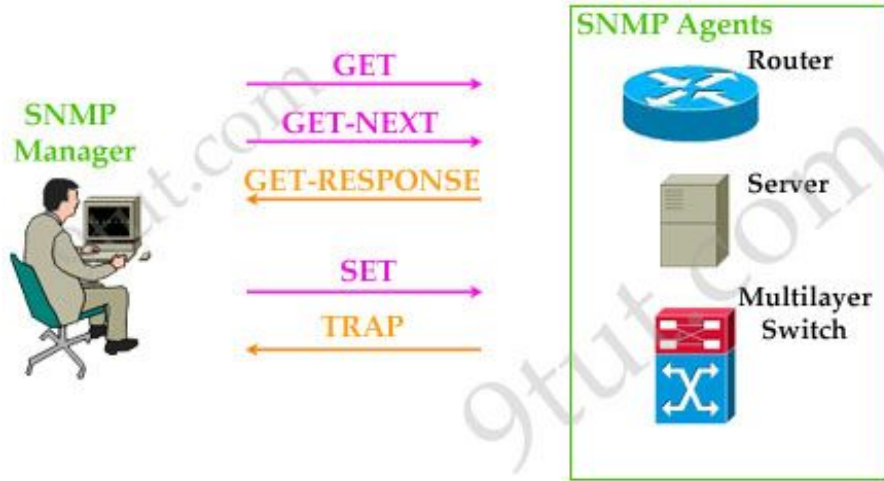   MIB is commonly shared between the Agent and Manager.
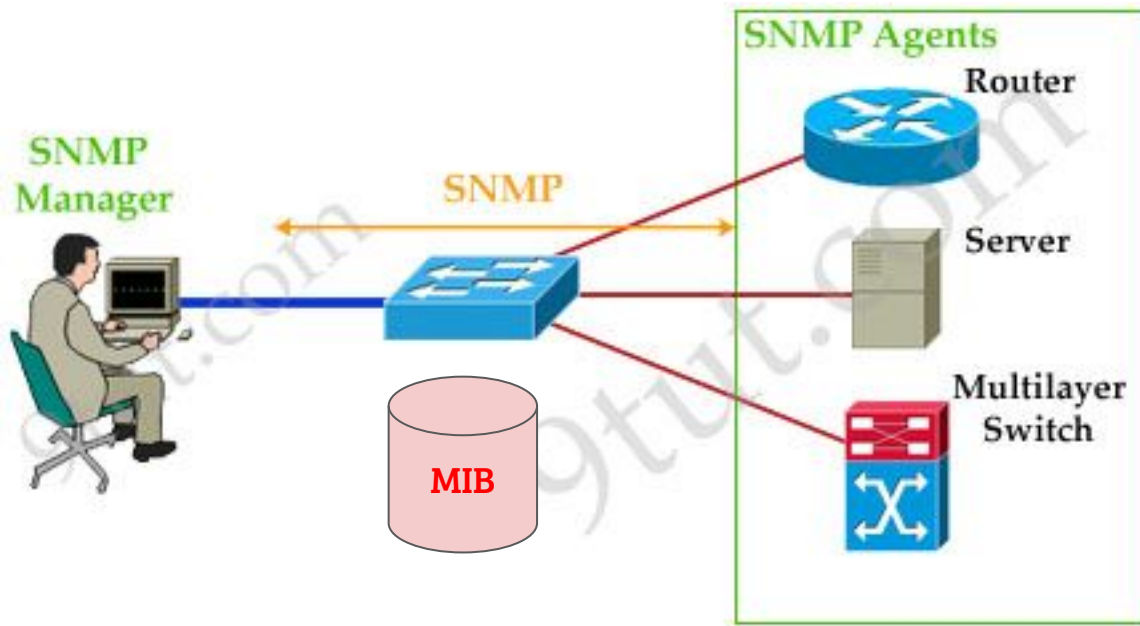
For example, in the topology above you want to monitor a router, a server and a Multilayer Switch. You can run SNMP Agent on all of them. Then on a PC you install a SNMP Manager software to receive monitoring information. SNMP is the protocol running between the Manager and Agent. SNMP communication between Manager and Agent takes place in form of messages. The monitoring process must be done via a MIB which is a standardized database and it contains parameters/objects to describe these networking devices (like IP addresses, interfaces, CPU utilization, …). Therefore the monitoring process now becomes the process of GET and SET the information from the MIB.

SNMP Messages

SNMP Messages are used to communicate between **the SNMP Manager and Agents.**

SNMP supports **five basic SNMP messages**:

1. **SNMP GET**

2. **SNMP GET-NEXT**

3. **SNMP GET-RESPONSE**

4. **SNMP SET**

5. **SNMP TRAP**

SNMP Manager

GET

GET-NEXT

GET-RESPONSE

SET

TRAP

SNMP Agents

Router

Server

Multilayer Switch

- **The GET messages** are sent by the SNMP Manager to retrieve information from the SNMP Agents .
- **The SET messages** are used by the SNMP Manager to modify or assign the value to the SNMP Agents.
- **GET-NEXT** retrieves the value of the next object in the MIB.
- **The GET-RESPONSE message** is used by the SNMP Agents to reply to GET and GET-NEXT messages.
- **TRAP messages** are initiated from the SNMP Agents to inform the SNMP Manager on the occurrence of an event.

File Transfer Protocol(FTP)

- File transfer protocol (FTP) is an Internet tool provided by TCP/IP.

- It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers.

- The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

The goals of FTP are:

- It encourages the direct use of remote computers.

- It shields users from system variations (operating system, directory structures, file structures, etc.)

- It promotes sharing of files and other types of data.

FTP protocol works on Client-Server Model:

Client-Server Model:

- A client initiates a connection to a remote server to transfer files. The client is responsible for sending commands, and the server responds to these commands.

- **Some of the commands are:**
    - get filename (retrieve the file from server)
    - mget filename (retrieve multiple files from the server)
    - ls (lists files available in the current directory of the server)

FTP Commands
FTP Replies
Data
Connection

FTP Client
on Client PC

FTP Server
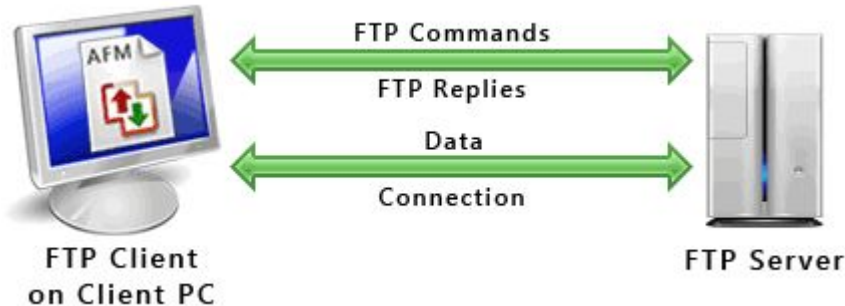
FTP operates in two primary modes: **Active and Passive**

Active Mode:

In this mode, **the client opens** a random port (known as the "data port") for data transfer, and the server connects to this port. The client's command port remains the same.

Passive Mode:

In passive mode, t**he server opens** a random data port, and the client connects to it for data transfer. This mode is often used when the client is behind a firewall or NAT, making it difficult for the server to initiate a connection.

Port Numbers:

FTP uses well-defined port numbers for communication. The default FTP control **port is 21**, and data transfers occur on various ports depending on whether active or passive mode is used.

Activity Time: Write the differences between FTP,SFTP,TFTP

FTP	
SFTP	
TFTP	

TELNET

What is Telnet?

- It is Command-line tool(Test-Oriented) to access the remote system.

- **TE**rmina**L NET**work, which is developed in 1969.

- TELNET follows **Client-server architecture.**

- Uses **PORT 23**

- It is **Fast** protocol

- **Cross-platform**

 - We can use TELNET in any operating system like **Windows,Linux,Mac.et**c.

Disadvantages :

- Not Secure (i.e Whatever the information transmitted from client and server is in the form of **clear text**)

- TELNET is basically the short form for TErminal NETwork.It is basically a TCP/IP protocol that is used for virtual terminal services and was mainly proposed by International Organization for Standards(ISO).
- It is a general-purpose client/server application program.
- This program enables the establishment of the connection to the remote system in such a way that the local system starts to appear as a terminal at the remote system.
- It is a standard TCP/IP protocol that is used for virtual terminal service.
- **In simple words, we can say that the telnet allows the user to log on to a remote computer. After logging on the user can use the services of the remote computer and then can transfer the results back to the local computer.**
- The TELNET was mainly designed at the time when most operating systems operate in the time-sharing environment. And in this type of environment, a large computer can support multiple users.
- Usually, the interaction between the computer and user occurs via terminal(It is a combination of keyboard, mouse, and monitor).
- TELNET makes the use of only one TCP/IP connection.

Logging

- The logging process can be further categorized into two parts:
  - Local Login
  - Remote Login
- **Local Login:** Whenever a user logs into its local system, it is known as local login.
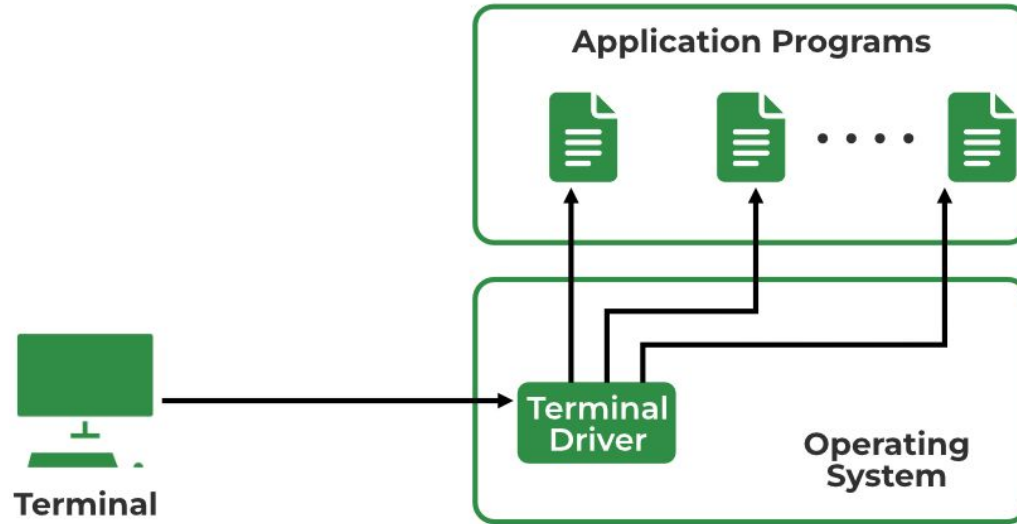
Local Login

The Procedure of Local Login

- Keystrokes are accepted by the terminal driver when the user types at the terminal.

- Terminal Driver passes these characters to OS.

- Now, OS validates the combination of characters and opens the required application.

2. Remote Login:

- Remote Login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer.

- With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.
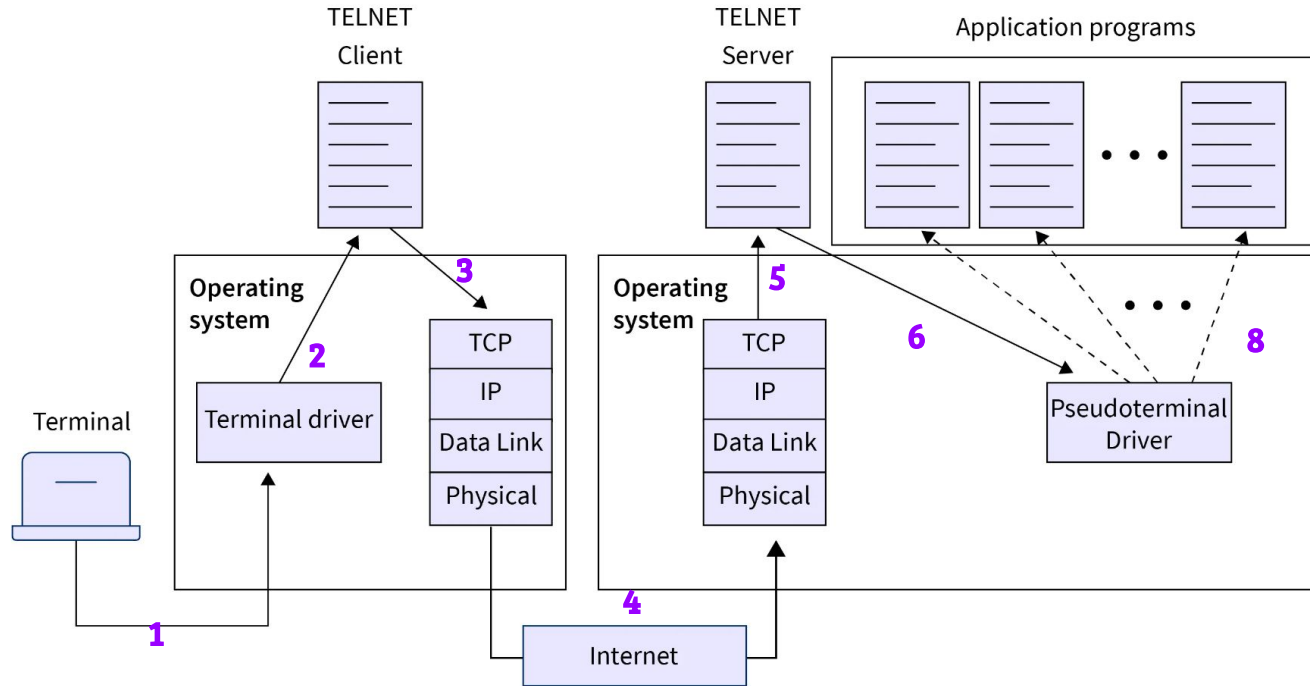
Remote Login in Logging

The Procedure of Remote Login

1. When the user types something on the local computer, the local operating system accepts the character.
2. The local computer does not interpret the characters, it will send them to the TELNET client.
3. TELNET client transforms these characters to a universal character set called **Network Virtual Terminal (NVT)** characters and it will pass them to the **local TCP/IP protocol Stack**.
4. Commands or text which are in the form of NVT, travel through the Internet and it will arrive at the TCP/IP stack at the remote computer.
5. Characters are then delivered to the operating system and later on passed to the TELNET server.
6. Then TELNET server changes those characters to characters that can be understandable by a remote computer.
7. The remote operating system receives characters from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
8. The operating system then passes the character to the appropriate application program.