REVA UNIVERSITY

Bengaluru, India

COMPUTER NETWORKS
M23DE0203
UNIT-IV

School of CSA/ MCA- 2nd Semester

Nagaraj C

www.reva.edu.in

UNIT IV

Introduction to Transport Layer

4th Layer

TRANSPORT LAYER SERVICES

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment.

Services Offered by Transport Layer

1. The transport layer provides reliable data transfer services such as segmentation, flow control, error detection, and retransmission, end-to-end communication between devices.

TRANSPORT LAYER SERVICES

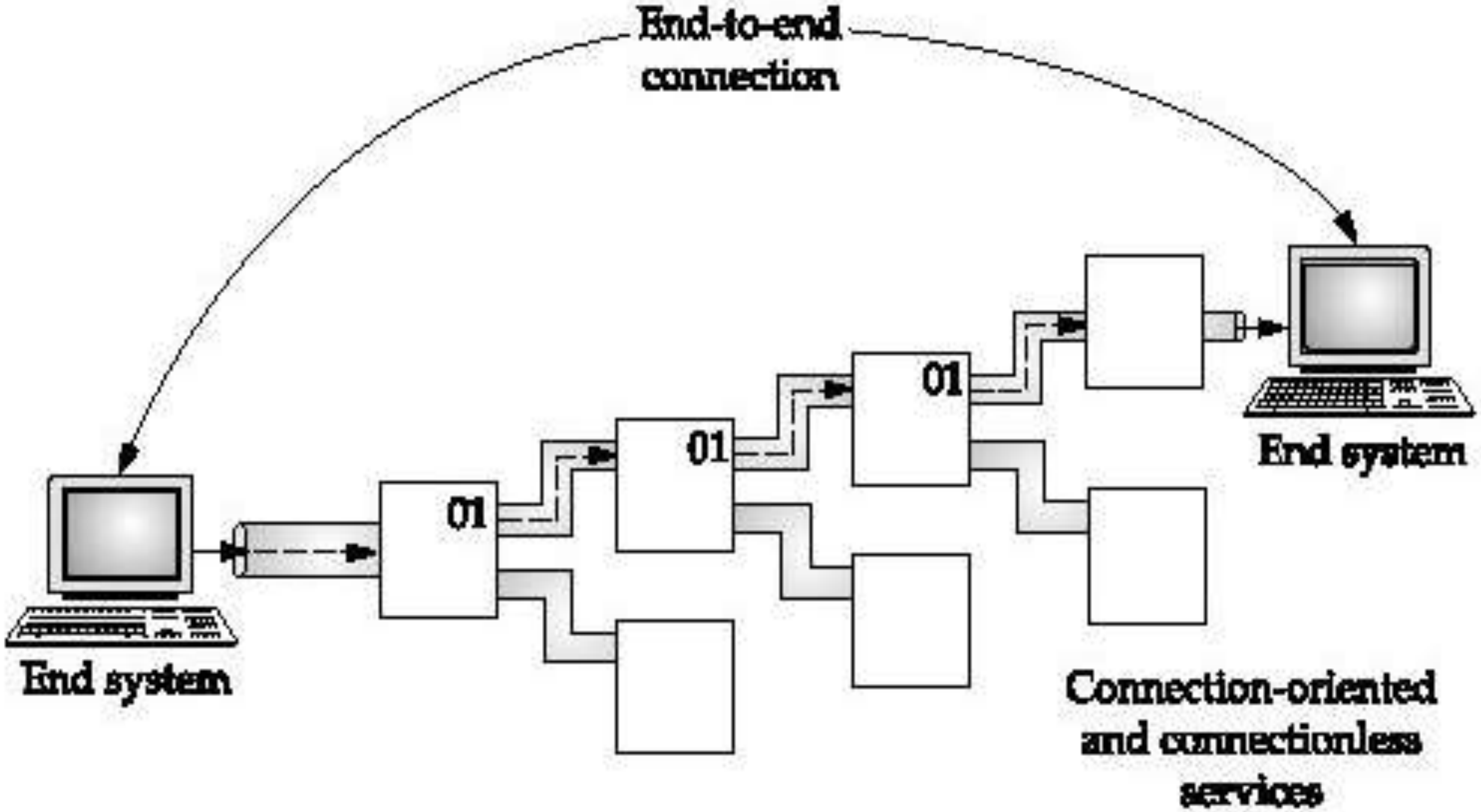
Services Offered by Transport Layer

The transport layer provides reliable data transfer services such as segmentation, flow control, error detection, and retransmission, end-to-end communication between devices.

1.End-to-end Connection between Hosts

The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures the reliable delivery of messages and is used in various applications.

UDP, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.


End-to-end connection
01
01
01
End system
End system
Connection-oriented and connectionless services

SERVICES OFFERED BY TRANSPORT LAYER

2.Flow Control

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model.

TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques.

It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

SERVICES OFFERED BY TRANSPORT LAYER

3. Multiplexing and Demultiplexing

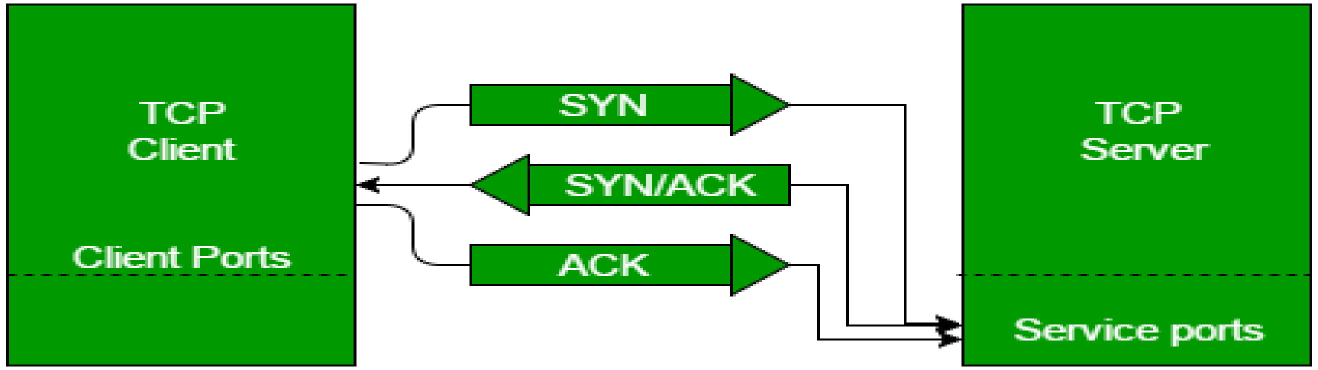
Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet. Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers.

Similarly, Demultiplexing(one to many) is required at the receiver side when the message is distributed into different processes. Transport receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.

SERVICES OFFERED BY TRANSPORT LAYER

4. Connection Establishment in TCP (3-Way Handshake)

1. TCP is a **connection-oriented protocol**.
   Before two devices (client and server) can communicate, they must **establish a reliable connection**.
2. This is done using the **3-Way Handshake** process.
3. The first computer connects to the second computer by sending a SYN packet to a specified port number.
4. If the second computer is listening, it will respond with a SYN/ACK.
5. When the first computer receives the SYN/ACK, it replies with an ACK packet.
6. After this, the two devices can communicate normally.



SERVICES OFFERED BY TRANSPORT LAYER

5.Connection Termination

1. In a TCP connection, we have two types of termination mechanisms:
2. In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.
3. In an unexpected connection release, either one TCP entity is forced to close the connection, or one user closes both directions of data transfer.

6. Reliable Data Delivery

1. The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.

WHAT ARE THE ELEMENTS OF TRANSPORT PROTOCOL?

To establish a reliable service between two machines on a network, transport protocols are implemented, which somehow resembles the data link protocols implemented at layer 2.

The major difference lies in the fact that the data link layer uses a physical channel between two routers while the transport layer uses a subnet.

Types of Service

The **transport layer** also determines the type of service provided to the users from the **session layer**. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer.

WHAT ARE THE ELEMENTS OF TRANSPORT PROTOCOL?

Error Control

Error detection and error recovery are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis. To control errors from lost or duplicate segments, the transport layer enables unique segment sequence numbers to the different packets of the message, creating virtual circuits, allowing only one virtual circuit per session.

Flow Control

The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. The transport layer enables a fast process to keep pace with a slow one. Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms are used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.

WHAT ARE THE ELEMENTS OF TRANSPORT PROTOCOL?

Connection Establishment/Release

The transport layer creates and releases the connection across the network. This includes a naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables us to establish and delete connections across the network to multiplex several message streams onto one communication channel.

Multiplexing/De multiplexing

The transport layer establishes a separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections.

When several connections are multiplexed, they call for demultiplexing at the receiving end.

WHAT ARE THE ELEMENTS OF TRANSPORT PROTOCOL?

Fragmentation and re-assembly

When the transport layer receives a large message from the session layer, it breaks the message into smaller units depending upon the requirement. This process is called fragmentation. Thereafter, it is passed to the network layer. Conversely, when the transport layer acts as the receiving process, it reorders the pieces of a message before reassembling them into a message.

Addressing

Transport Layer deals with addressing or labelling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame, so the receiving device knows which process it has been sent from. This helps in keeping track of multiple-message conversations. Ports or sockets address multiple conservations in the same location.

TRANSPORT LAYER PROTOCOLS

The transport layer is the fourth layer in the OSI model and the second layer in the TCP/IP model. The transport layer provides with end to end connection between the source and the destination and reliable delivery of the services. Therefore transport layer is known as the end-to-end layer.

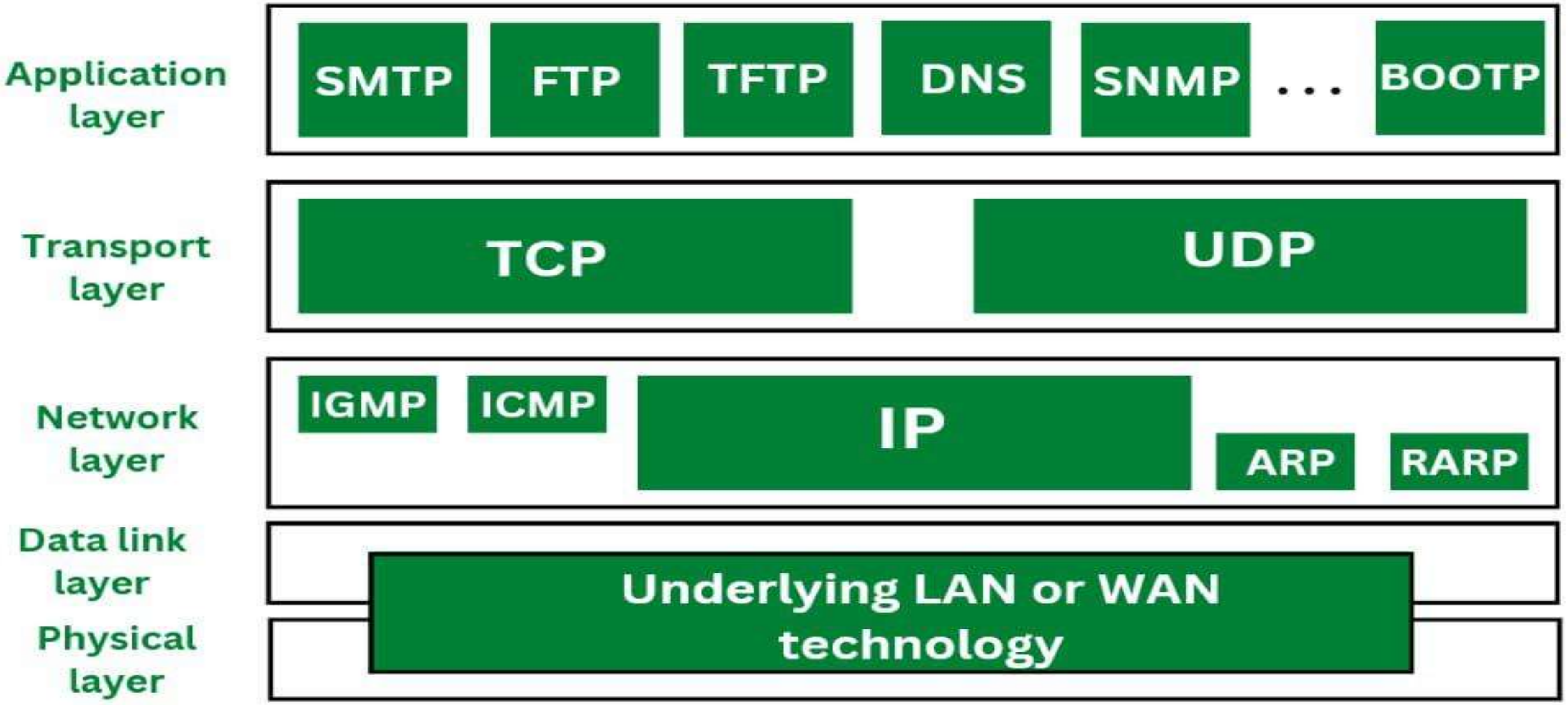
The transport layer takes the services from its upward layer which is the application layer and provides it to the network layer. Segment is the unit of data encapsulation at the transport layer.

Functions of Transport Layer

1. The process to process delivery
2. End-to-end connection between devices
3. Multiplexing and Demultiplexing
4. Data integrity and error Correction
5. Congestion Control
6. Flow Control

TRANSPORT LAYER PROTOCOLS

The transport layer is represented majorly by TCP and UDP protocols. Today almost all operating systems support multiprocessing multi-user environments. This transport layer protocol provides connections to the individual ports. These ports are known as protocol ports. Transport layer protocols work above the IP protocols and deliver the data packets from IP serves to destination port and from the originating port to destination IP services.



TRANSPORT LAYER PROTOCOLS-UDP

UDP stands for User Datagram Protocol. User Datagram Protocol provides a nonsequential transmission of data. It is a connectionless transport protocol.

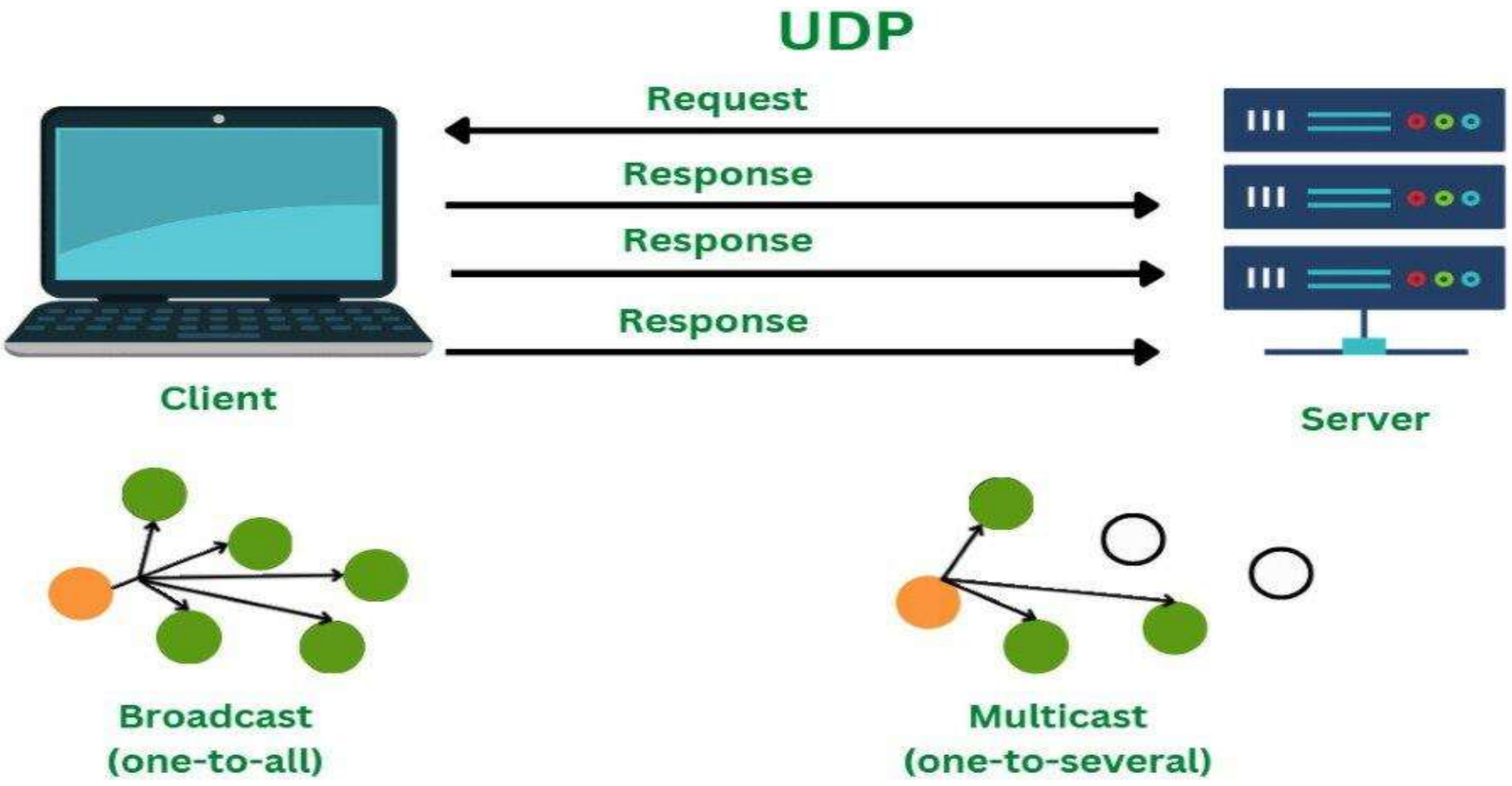
UDP protocol is used in applications where the speed and size of data transmitted is considered as more important than the security and reliability.

User Datagram is defined as a packet produced by User Datagram Protocol.

UDP protocol adds checksum error control, transport level addresses, and information of length to the data received from the layer above it.

Services provided by User Datagram Protocol(UDP) are connectionless service, faster delivery of messages, checksum, and process-to-process communication.

TRANSPORT LAYER PROTOCOLS-UDP

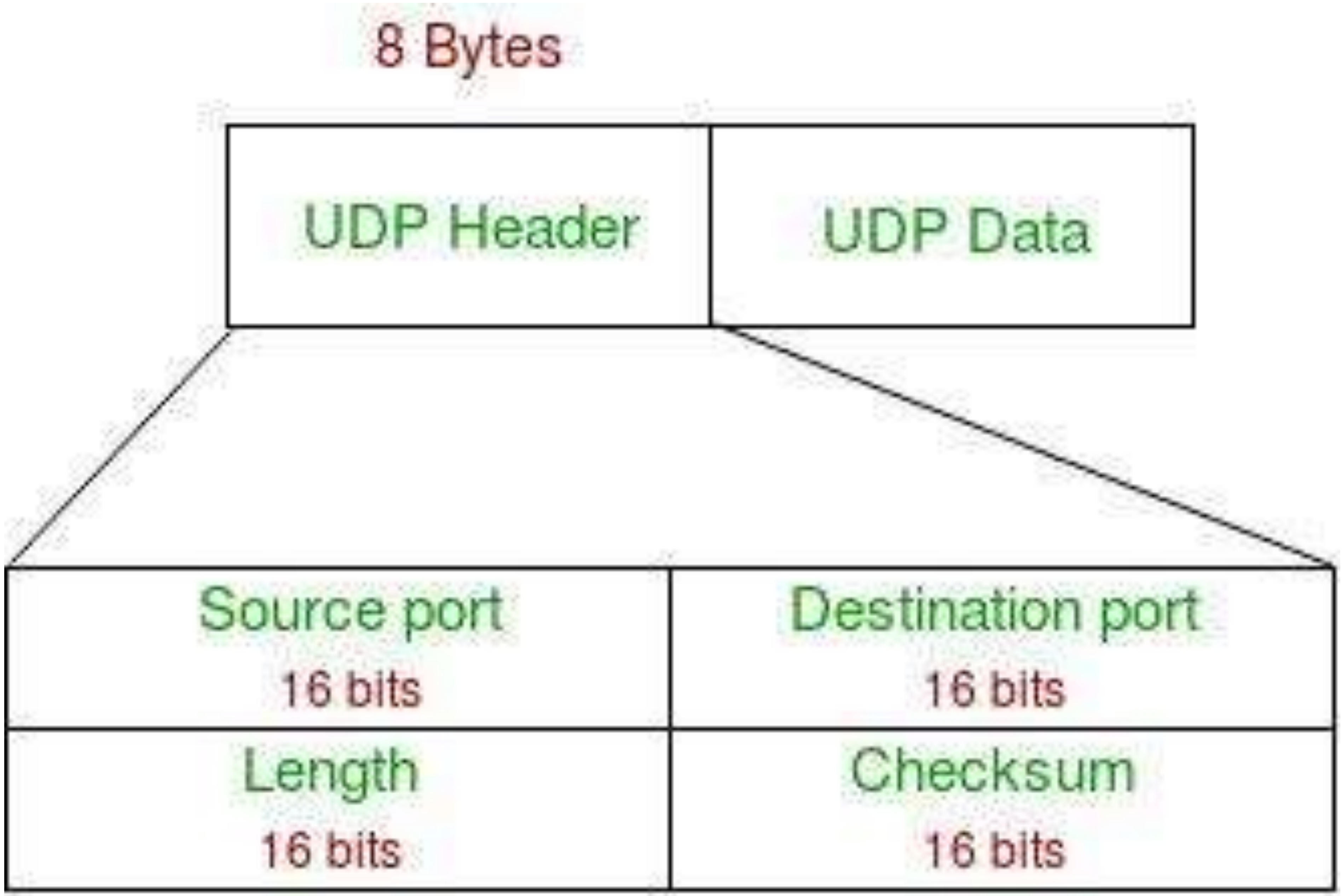


UDP SEGMENT

While the TCP header can range from 20 to 60 bytes, the UDP header is a fixed, basic 8 bytes. All required header information is contained in the first 8 bytes, with data making up the remaining portion. Because UDP port number fields are 16 bits long, the range of possible port numbers is defined as 0 to 65535, with port 0 being reserved.

1. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
2. **Destination Port:** This 2-byte element is used to specify the packet's destination port.
3. **Length:** The whole length of a UDP packet, including the data and header. The field has sixteen bits.
4. **Cheksum:** The checksum field is two bytes long. The data is padded with zero octets at the end (if needed) to create a multiple of two octets. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header containing information from the IP header, and the data.

UDP SEGMENT



8 Bytes

UDP Header	UDP Data

Source port 16 bits	Destination port 16 bits
Length 16 bits	Checksum 16 bits

Advantages of UDP

1. UDP also provides multicast and broadcast transmission of data.
2. UDP protocol is preferred more for small transactions such as DNS lookup(DNS lookup = name-to-number translation).
3. It is a connectionless protocol, therefore there is no compulsion to have a connection-oriented network.
4. UDP provides fast delivery of messages.

Disadvantages of UDP

1. In UDP protocol there is no guarantee that the packet is delivered.
2. UDP protocol suffers from worse packet loss.
3. UDP protocol has no congestion control mechanism.
4. UDP protocol does not provide the sequential transmission of data.

Advantages of UDP

1. UDP also provides multicast and broadcast transmission of data.
2. UDP protocol is preferred more for small transactions such as DNS lookup(DNS lookup = name-to-number translation).
3. It is a connectionless protocol, therefore there is no compulsion to have a connection-oriented network.
4. UDP provides fast delivery of messages.

Disadvantages of UDP

1. In UDP protocol there is no guarantee that the packet is delivered.
2. UDP protocol suffers from worse packet loss.
3. UDP protocol has no congestion control mechanism.
4. UDP protocol does not provide the sequential transmission of data.

TRANSPORT LAYER PROTOCOLS-TCP

TCP stands for Transmission Control Protocol. TCP protocol provides transport layer services to applications.

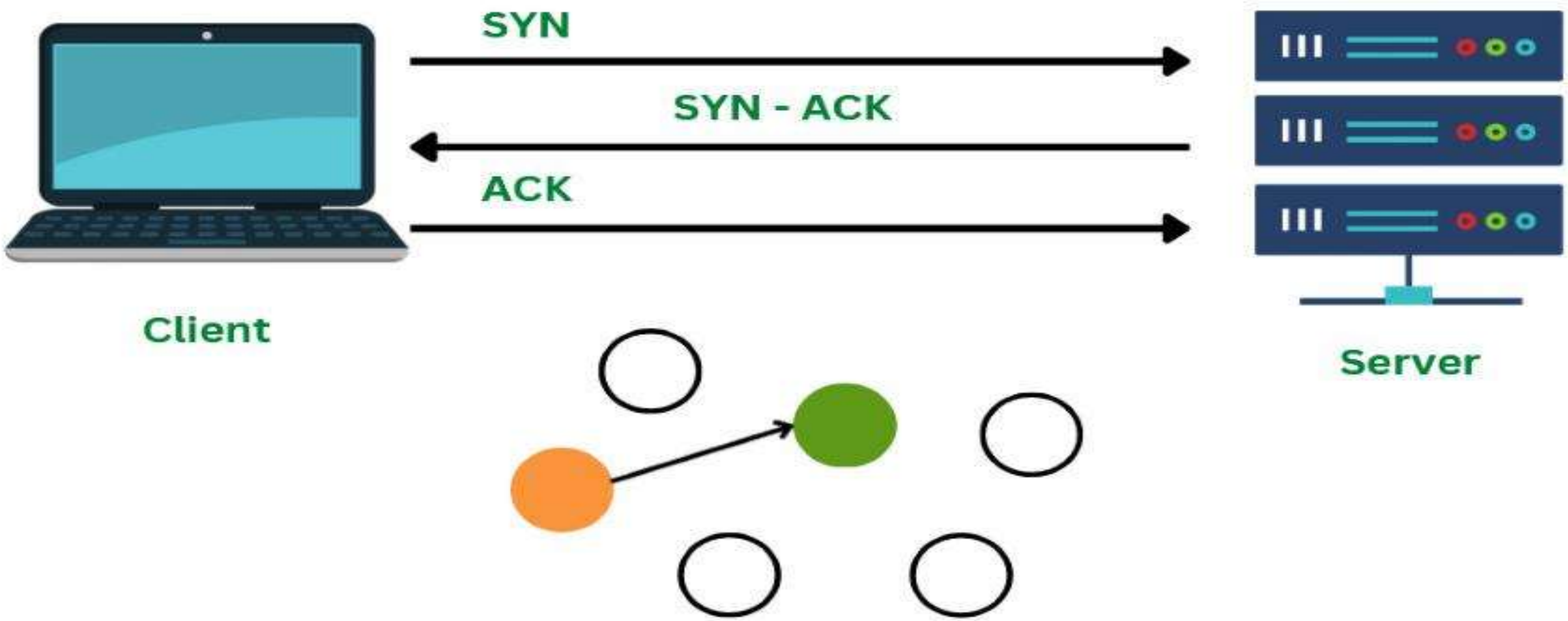
TCP protocol is a connection-oriented protocol. A secured connection is being established between the sender and the receiver.

For a generation of a secured connection, a virtual circuit is generated between the sender and the receiver.

The data transmitted by TCP protocol is in the form of continuous byte streams. A unique sequence number is assigned to each byte. With the help of this unique number, a positive acknowledgment is received from receipt.

If the acknowledgment is not received within a specific period the data is retransmitted to the specified destination.

TCP

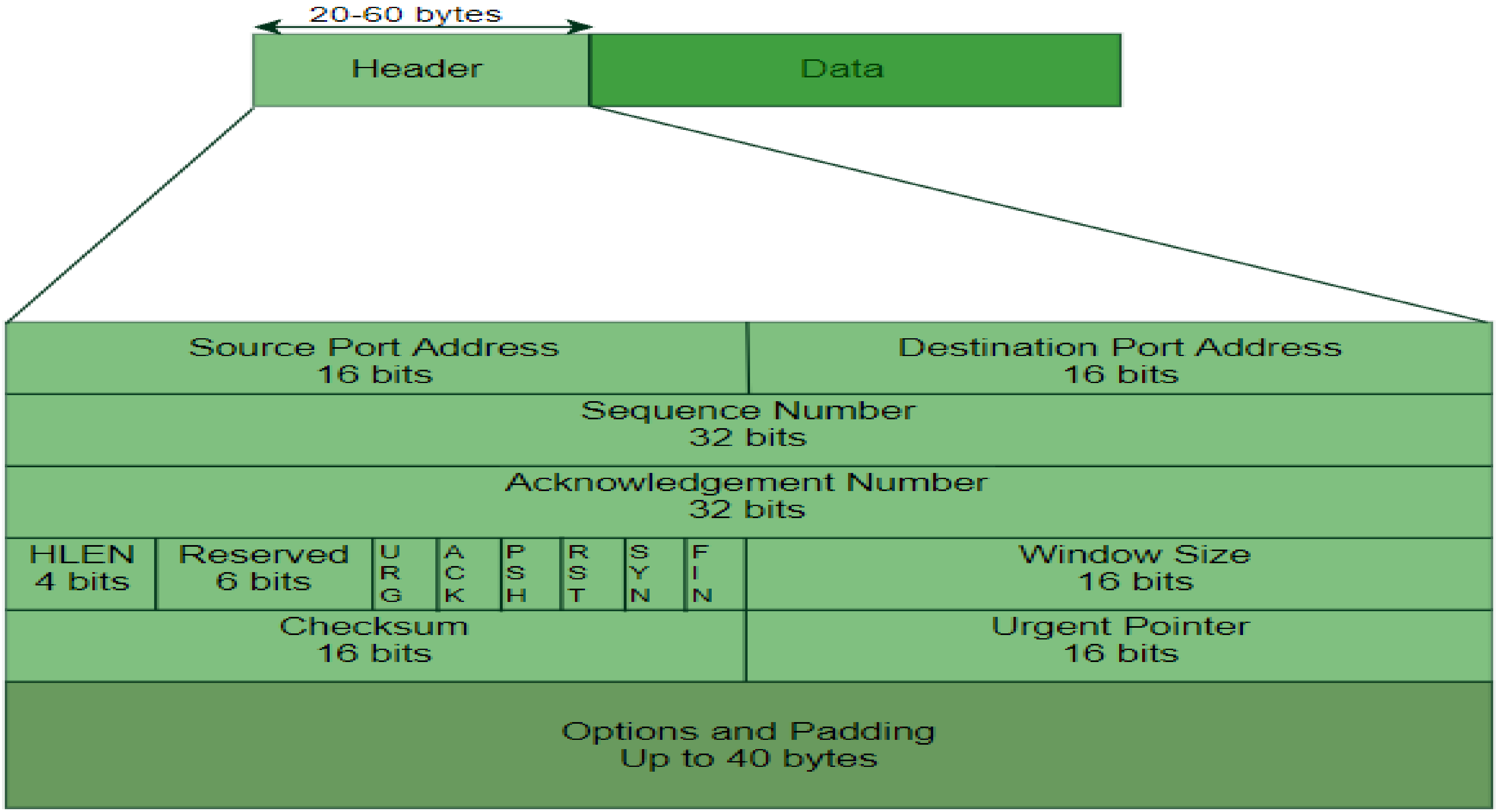


Unicast
(one-to-one)

TRANSPORT LAYER PROTOCOLS-TCP

TCP Segment

A TCP segment's header may have 20–60 bytes. The options take about 40 bytes. A header consists of 20 bytes by default, although it can contain up to 60 bytes.



20-60 bytes

Header

Data

Source Port Address
16 bits

Destination Port Address
16 bits

Sequence Number
32 bits

Acknowledgement Number
32 bits

HLEN
4 bits

Reserved
6 bits

URG

ACK

PSH

RST

SYN

FIN

Window Size
16 bits

Checksum
16 bits

Urgent Pointer
16 bits

Options and Padding
Up to 40 bytes

TRANSPORT LAYER PROTOCOLS-TCP

1. **Source Port Address:** The port address of the programme sending the data segment is stored in the 16-bit field known as the source port address.

2. **Destination Port Address:** The port address of the application running on the host receiving the data segment is stored in the destination port address, a 16-bit field.

3. **Sequence Number:** The sequence number, or the byte number of the first byte sent in that specific segment, is stored in a 32-bit field. At the receiving end, it is used to put the message back together once it has been received out of sequence.

4. **Acknowledgement Number** : The acknowledgement number, or the byte number that the recipient anticipates receiving next, is stored in a 32-bit field called the acknowledgement number. It serves as a confirmation that the earlier bytes were successfully received.

TRANSPORT LAYER PROTOCOLS-TCP

5.Header Length (HLEN): This 4-bit field stores the number of 4-byte words in the TCP header, indicating how long the header is.

6.Control flags: These are six 1-bit control bits that regulate flow control, method of transfer, connection abortion, termination, and establishment. They serve the following purposes:

1. **Urgent:** This pointer is legitimate
2. **ACK:** The acknowledgement number (used in cumulative acknowledgement cases) is valid.
3. **PSH:** Push request
4. **RST:** Restart the link.
5. SYN: Sequence number synchronisation
6. **FIN:** Cut off the communication
7. **Window size:** This parameter provides the sender TCP's window size in bytes.

TRANSPORT LAYER PROTOCOLS-TCP

7.Checksum: The checksum for error control is stored in this field. Unlike UDP, it is required for TCP.

8.Urgent pointer: This field is used to point to data that must urgently reach the receiving process as soon as possible. It is only valid if the URG control flag is set. To obtain the byte number of the final urgent byte, the value of this field is appended to the sequence number.

TRANSPORT LAYER PROTOCOLS-TCP

Advantages of TCP

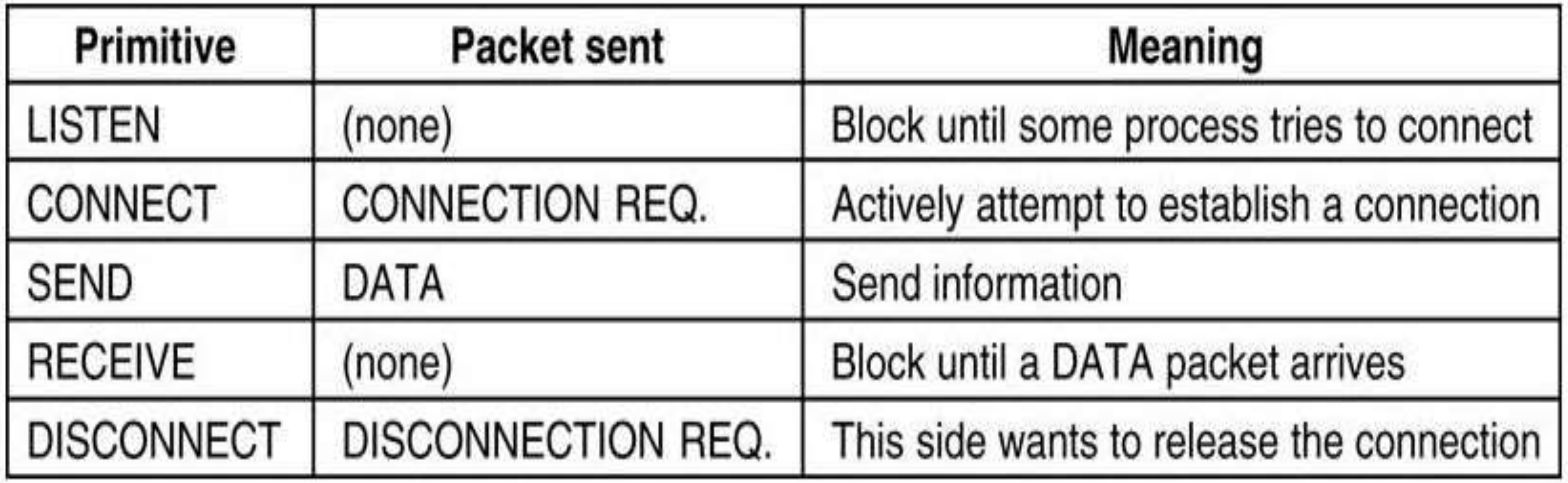
1. TCP supports multiple routing protocols.
2. TCP protocol operates independently of that of the operating system.
3. TCP protocol provides the features of error control and flow control.
4. TCP provides a connection-oriented protocol and provides the delivery of data.

Disadvantages of TCP

1. TCP protocol cannot be used for broadcast or multicast transmission.
2. TCP protocol has no block boundaries.
3. No clear separation is being offered by TCP protocol between its interface, services, and protocols.
4. In TCP/IP replacement of protocol is difficult.

TRANSPORT SERVICE PRIMITIVES

Instructions



Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

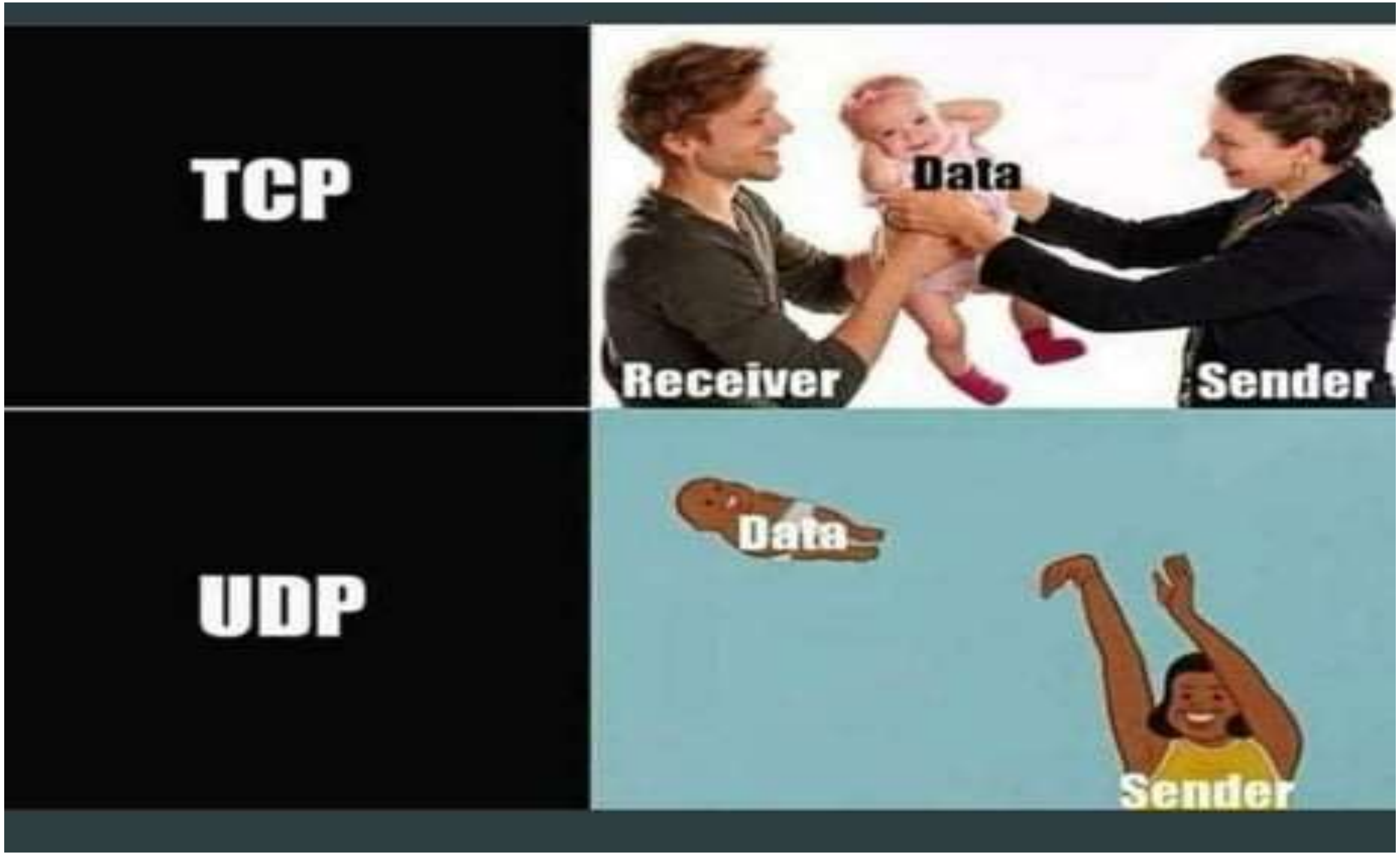
DIFFERENCES BETWEEN TCP AND UDP

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.

DIFFERENCES BETWEEN TCP AND UDP

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs , FTP , SMTP and Telnet .	UDP is used by DNS , DHCP , TFTP, SNMP , RIP , and VoIP .

PICTORIAL WAY TO SAY TCP & UDP



DOMAIN NAME SYSTEM (DNS)

1. DNS is a hierarchical and distributed naming system that translates domain names into IP addresses.
2. When you type a domain name like www.facebook.com into your browser, DNS ensures that the request reaches the correct server by resolving the domain to its corresponding IP address.
3. Without DNS, we'd have to remember the numerical IP address of every website we want to visit, which is highly impractical.

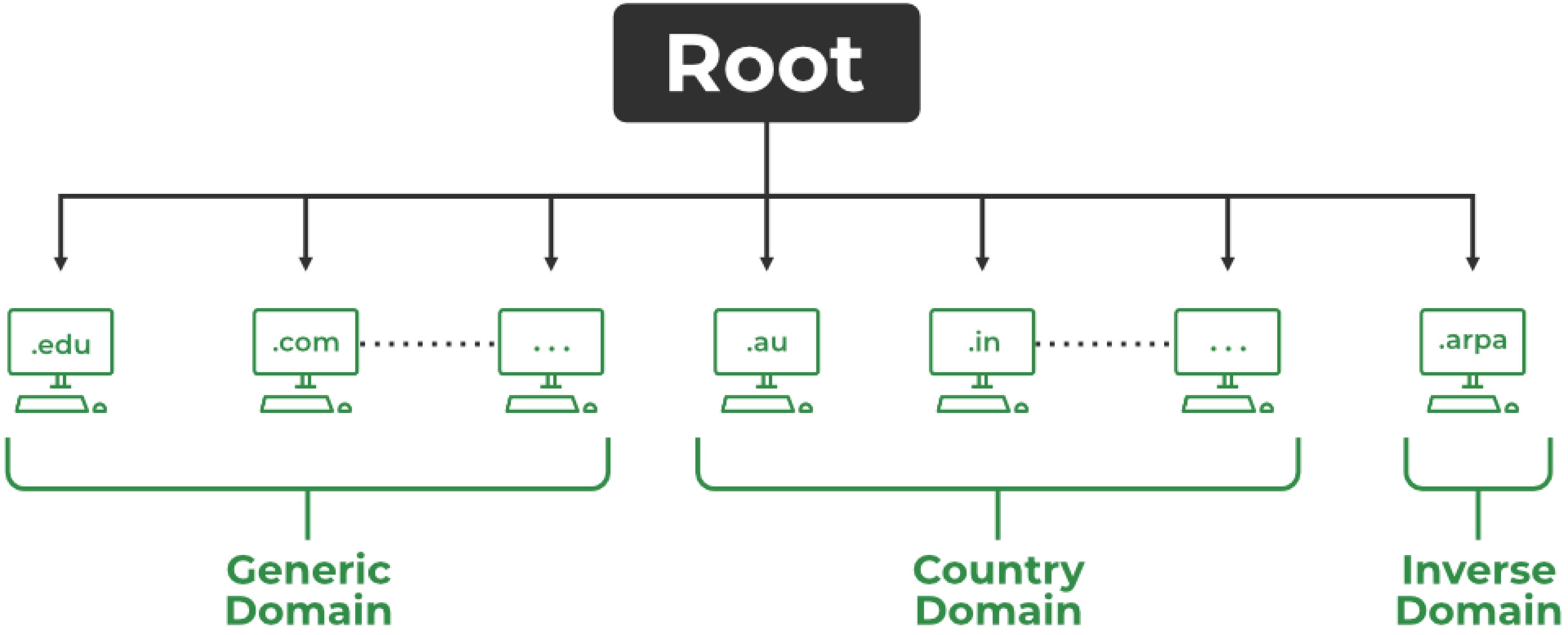
DOMAIN NAME SYSTEM (DNS)

Types of Domains

1. DNS helps manage a wide variety of domain types to organize the vast number of websites on the internet. Here are the primary categories:
2. **Generic Domains:** These include top-level domains like .com, .org, .net and .edu. These are widely used and recognized across the world.
3. **Country Code Domains:** These domains represent specific countries or regions, such as .in for India, .us for the United States, .uk for the United Kingdom and .jp for Japan.
4. **Inverse Domains:** Used for reverse DNS lookups, these domains help map IP addresses back to domain names. Reverse DNS lookups are useful for diagnostics and security purposes, ensuring that the source of network traffic is legitimate. So DNS can provide both the mapping for example to find the IP addresses of facebook.com then we have to type

DOMAIN NAME SYSTEM (DNS)

Types of Domains



DOMAIN NAME SYSTEM (DNS)

Domain Name Server

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

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

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

DOMAIN NAME SYSTEM (DNS)

DNS Lookup

1. DNS_Lookup, also called DNS Resolution, is the process of translating a human-readable domain name (like www.example.com) into its corresponding IP address (like 192.0.2.1), which computers use to locate and communicate with each other on the internet. It allows users to access websites easily using names instead of remembering numeric IP addresses.
2. DNS Lookup starts when a user types a domain name into their browser.
3. The query goes through a series of servers: the DNS resolver, Root server, TLD server and authoritative server.
4. Each server plays a role in finding the correct IP address for the domain.
5. Once the IP address is found, the browser connects to the website's server and loads the page.

DOMAIN NAME SYSTEM (DNS)

DNS Resolver

1. DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution.
2. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names that are very much friendly to the user and that also resolves the problem of remembering IP Address.

ELECTRONIC MAIL

Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email:

1. An email address: This is a unique identifier for each user, typically in the format of name@domain.com.
2. An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.
3. An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.

ELECTRONIC MAIL

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service.

ELECTRONIC MAIL

Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA) :** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

2. **Message Transfer Agent (MTA) :** MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.

ELECTRONIC MAIL

Components of E-Mail System :

3.Mailbox : It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

4.Spool file : This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

ELECTRONIC MAIL

Services provided by E-mail system :

1. **Composition -** The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
2. **Transfer -** Transfer means sending procedure of mail i.e. from the sender to recipient.
3. **Reporting -** Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
4. **Displaying -** It refers to present mail in form that is understand by the user.
5. **Disposition -** This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

ELECTRONIC MAIL

To send an email:

1. Compose a new message in your email client.
2. Enter the recipient's email address in the "To" field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click "Send" to deliver the message to the recipient's email server.
7. Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients, and reply, reply all, and forward options to manage the conversation.

ELECTRONIC MAIL

Advantages of email:

1. Convenient and fast communication with individuals or groups globally.
2. Easy to store and search for past messages.
3. Ability to send and receive attachments such as documents, images, and videos.
4. Cost-effective compared to traditional mail and fax.
5. Available 24/7.

ELECTRONIC MAIL

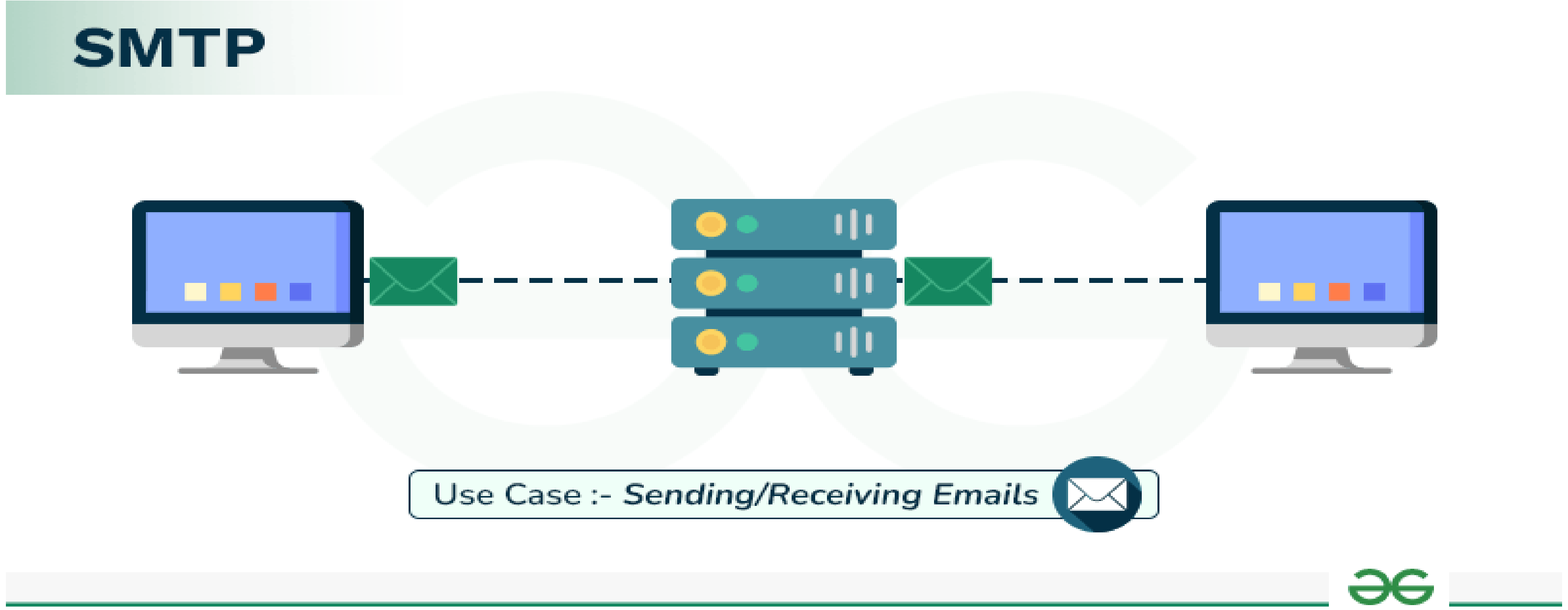
Disadvantages of email:

1. Risk of spam and phishing attacks.
2. Overwhelming amount of emails can lead to information overload.
3. Can lead to decreased face-to-face communication and loss of personal touch.
4. Potential for miscommunication due to lack of tone and body language in written messages.
5. Technical issues, such as server outages, can disrupt email service.
6. It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

1. **Simple Mail Transfer Protocol (SMTP)** is an application layer protocol used for exchanging email messages between servers. It is essential in the email communication process and operates at the application layer of the TCP/IP stack.

2. To send an email, the client opens a TCP connection to the SMTP server. The server, which is always listening on port 25, initiates the connection as soon as it detects a client. Once the TCP connection is established, the client sends the email across the connection.



SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Types of SMTP Protocol

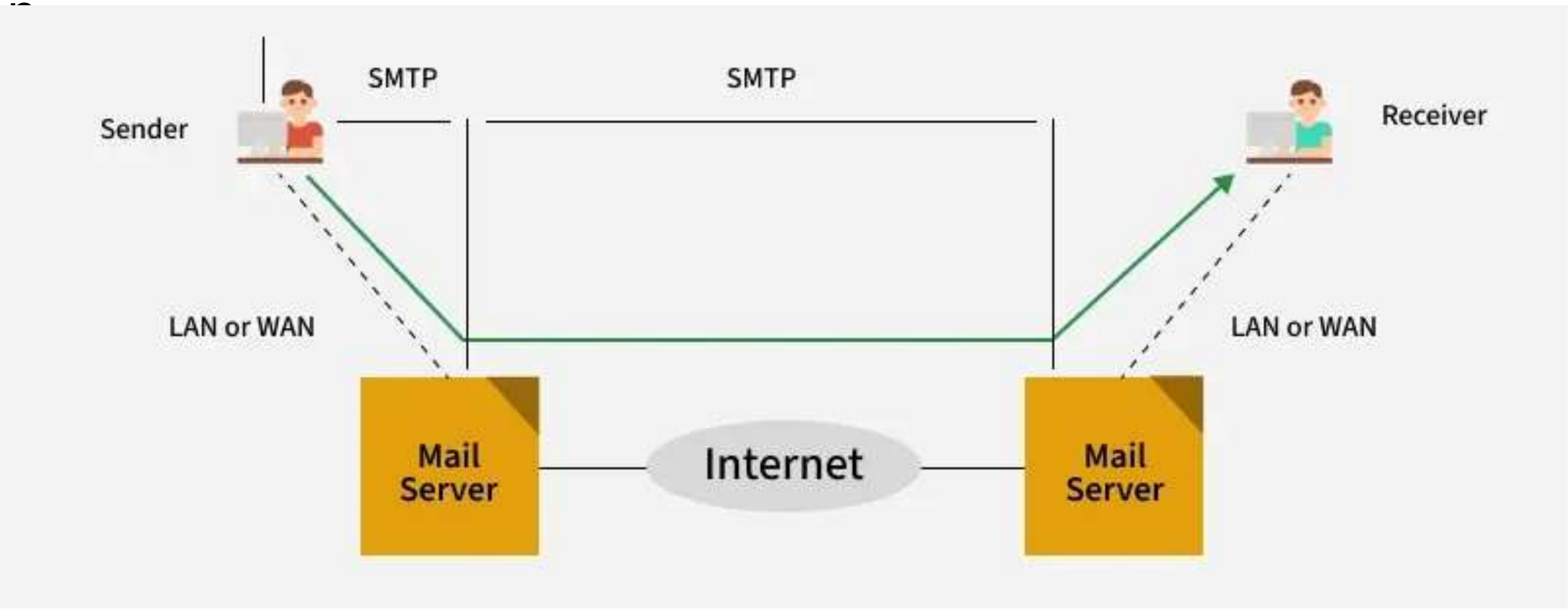
1. The **SMTP model** supports two types of email delivery methods: **end-to-end** and **store-and-forward**.

2. **End-to-end** delivery is used between organizations. In this method, the email is sent directly from the sender's SMTP client to the recipient's SMTP server without passing through intermediate servers.

3. **Store-and-forward** is used within organizations that have TCP/IP and SMTP-based networks. In this method, the email may pass through several intermediate servers (Message Transfer Agents, or MTAs) before reaching the recipient.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

4.With **end-to-end** delivery, the SMTP client waits until the email is successfully copied to the recipient's SMTP server before sending it. This is different from the **store-and-forward** method, where the email might stop at multiple intermediate servers before reaching its destination. In store-and-forward systems, the sender is notified as soon as the email reaches the first server, not the final destinatio



SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Components of SMTP

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 receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
3. **Mail Transfer Agent (MTA):** It is 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.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

How does SMTP Work?

1. Sending Email:

1. When a user wants to send an email, they use a **User Agent (UA)**, like Outlook or Gmail.
2. The email is handed over to the **MTA**, which is responsible for transferring the email to the recipient's mail server.

2. SMTP Client and Server:

1. **Sender-SMTP (Client)**: The email sender's MTA initiates the connection to the recipient's MTA (Receiver-SMTP).
2. **Receiver-SMTP (Server)**: The receiving MTA listens for incoming connections and receives the email from the sender-SMTP.
3. This communication happens over **TCP port 25**.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

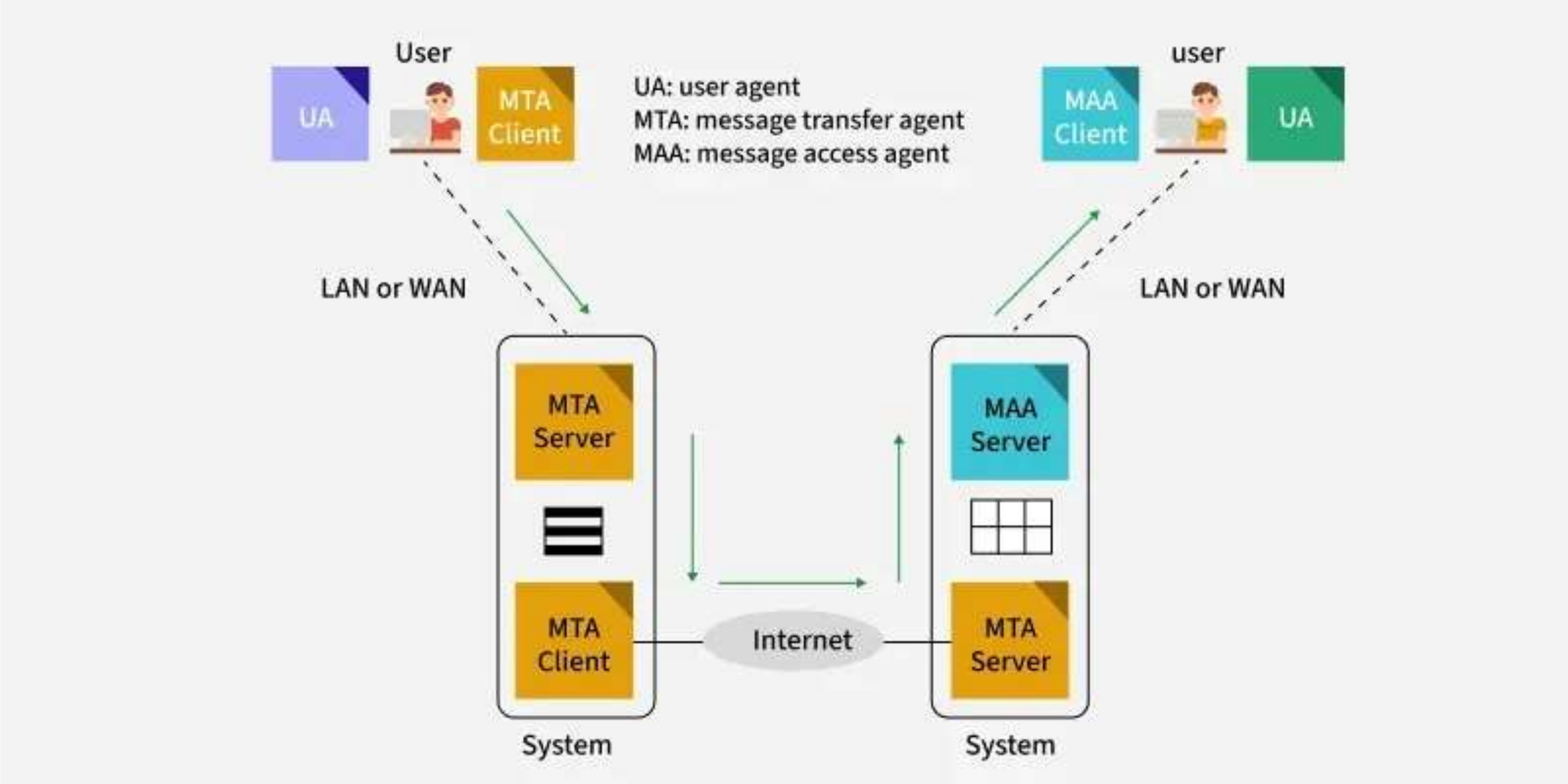
3. Relays and Gateways:

1. **Relays**: In some cases, the email may pass through several intermediate MTAs before reaching the destination server. These MTAs act as **relays**.
2. **Gateways**: If the sending and receiving systems use different email protocols (e.g., SMTP and non-SMTP), an **email gateway** can convert the email to the appropriate format for delivery.

4. Email Delivery:

1. The sender's **MTA** sends the email to the **receiver's MTA**, either directly or through relays.
2. The **MTA** uses the **SMTP** protocol to transfer the message. Once it's delivered to the destination MTA, the email is placed in the recipient's mailbox.
3. The recipient's **User Agent (UA)** can then download the email.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)



UA: user agent
MTA: message transfer agent
MAA: message access agent

WORLD WIDE WEB (WWW)

1. The World Wide Web (WWW), often called the Web, is a system of interconnected webpages and information that you can access using the Internet. It was created to help people share and find information easily, using links that connect different pages together. The Web allows us to browse websites, watch videos, shop online, and connect with others around the world through our computers and phones.

2. All public websites or web pages that people may access on their local computers and other devices through the internet are collectively known as the World Wide Web or W3. Users can get further information by navigating to links interconnecting these pages and documents. This data may be presented in text, picture, audio, or video formats on the internet.

WORLD WIDE WEB (WWW)

Key Parts of the Web

The Web has three main building blocks that make it work:

1. **URL (Uniform Resource Locator):** This is the address of a webpage, like https://www.example.com./ It tells your browser exactly where to find the page.
2. **HTTP (Hypertext Transfer Protocol):** This is the set of rules that lets your browser and the server talk to each other to send and receive webpages.
3. **HTML (Hypertext Markup Language):** This is the code that tells browsers how to display a webpage, including where to put text, pictures, and links.

WORLD WIDE WEB (WWW)

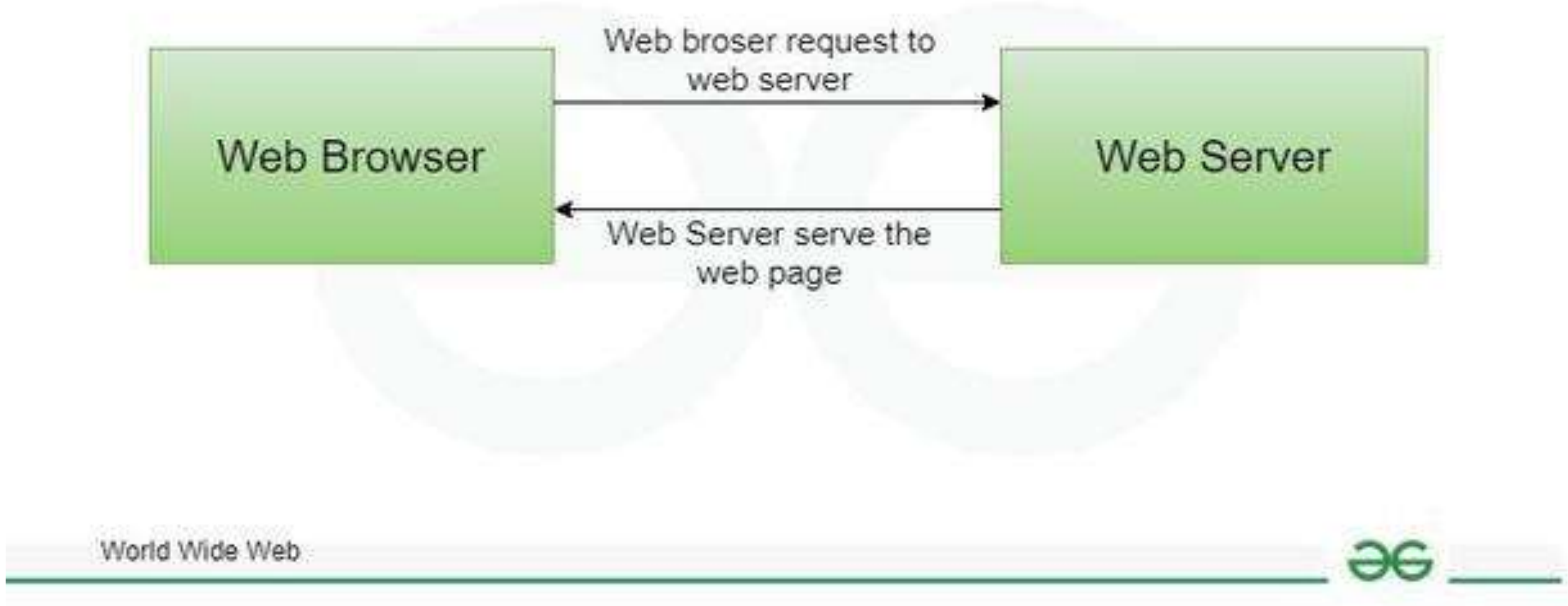
Working of World Wide Web(WWW)

1. A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal.

2. The below diagram indicates how the Web operates just like client-server architecture of the internet. When users request web pages or other information, then the web browser of your system request to the server for the information and then the web server provide requested services to web browser back and finally the requested service is utilized by the user who made the request.

WORLD WIDE WEB (WWW)

Working of World Wide Web(WWW)


Web broser request to web server
Web Browser
Web Server
Web Server serve the web page

World Wide Web

WORLD WIDE WEB (WWW) VS INTERNET

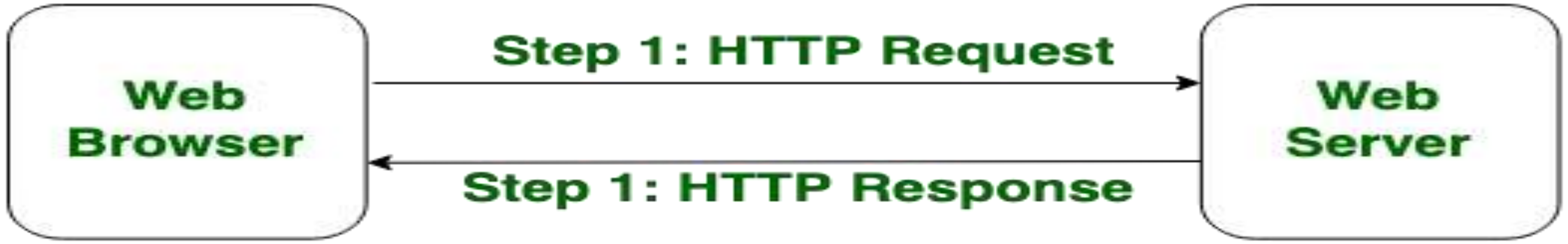
Aspect	World Wide Web	Internet
What It Is	A collection of webpages and websites you access with a browser.	A global network connecting computers.
Started	1989 by Tim Berners-Lee at CERN.	1960s as ARPANET.
Purpose	To share and explore information like text, images, and videos.	To connect devices and share data.
How You Use It	Through browsers like Chrome or Firefox.	Through any connected device for email, apps, etc.
Example	Visiting a website like Wikipedia.	Sending an email or streaming a video.

DIFFERENCE BETWEEN STATIC AND DYNAMIC WEB PAGES

1. There are two basic methods of web design: static and dynamic web pages. Users access static web pages, which present the same content every time they are viewed. On the other hand, dynamic webpages create content instantly in response to user input and present customized or updated information.

What are Static Web Pages?

1. Static Web pages are very simple. It is written in languages such as HTML, JavaScript, CSS, etc. For static web pages when a server receives a request for a web page, then the server sends the response to the client without doing any additional process. These web pages are seen through a web browser.
2. In static web pages, Pages will remain the same until someone changes it manually.



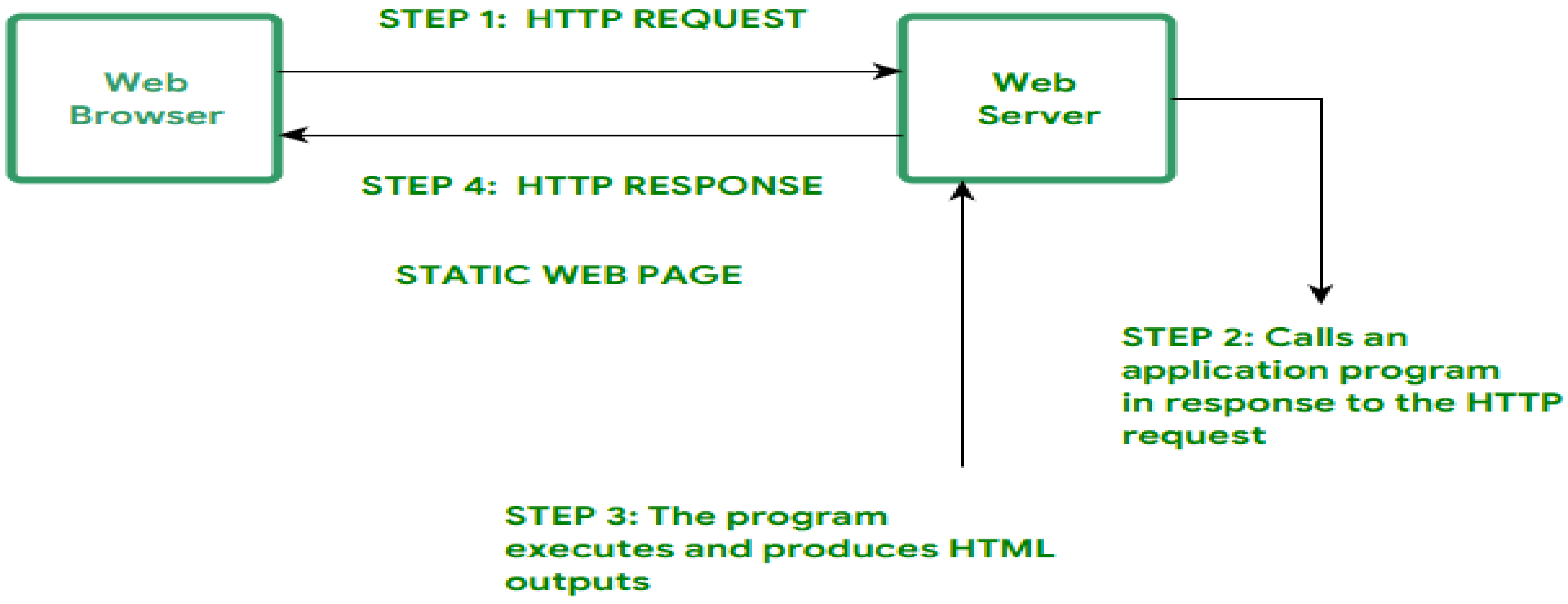
Static Web Page

DIFFERENCE BETWEEN STATIC AND DYNAMIC WEB PAGES

What are Dynamic Web Pages?

Dynamic Web Pages are written in languages such as CGI, AJAX, ASP, ASP.NET, etc. In dynamic web pages, the Content of pages is different for different visitors. It takes more time to load than the static web page.

Dynamic web pages are used where the information is changed frequently, for example, stock prices, weather information, etc.


STEP 1: HTTP REQUEST
Web Browser
Web Server
STEP 4: HTTP RESPONSE
STATIC WEB PAGE
STEP 2: Calls an application program in response to the HTTP request
STEP 3: The program executes and produces HTML outputs

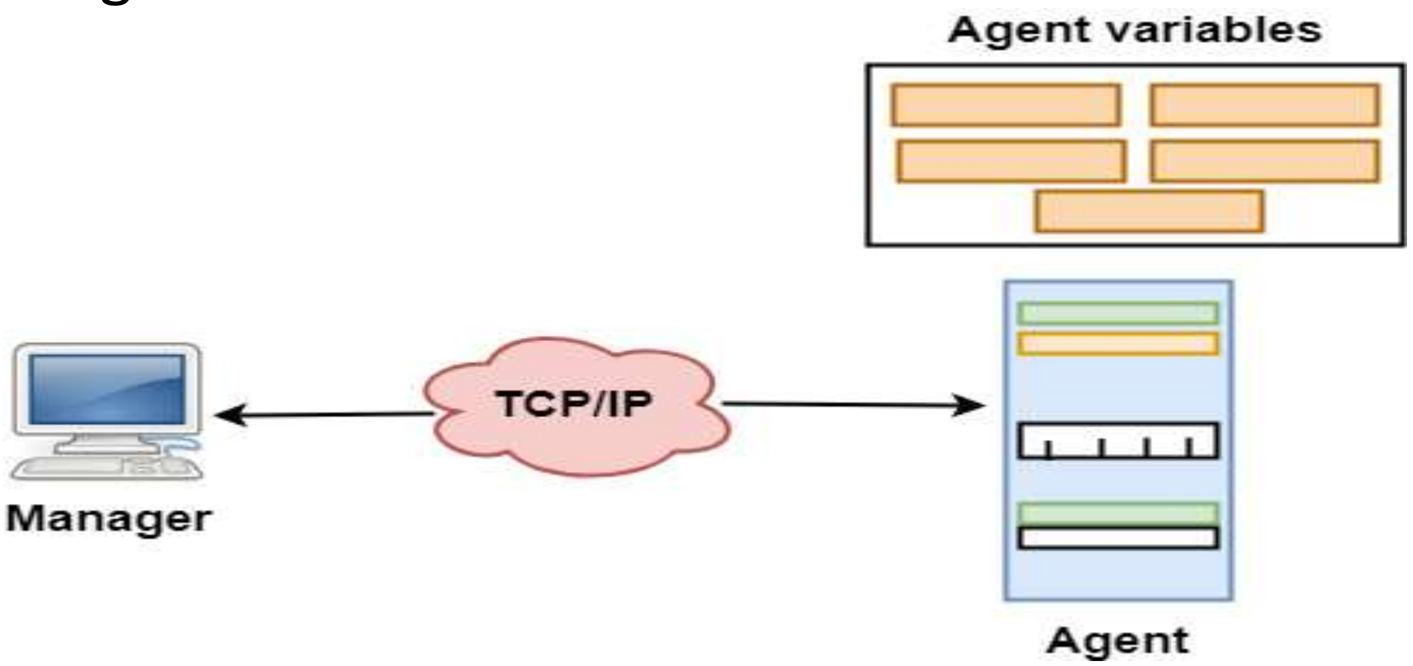
Dynamic web page

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

- 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.

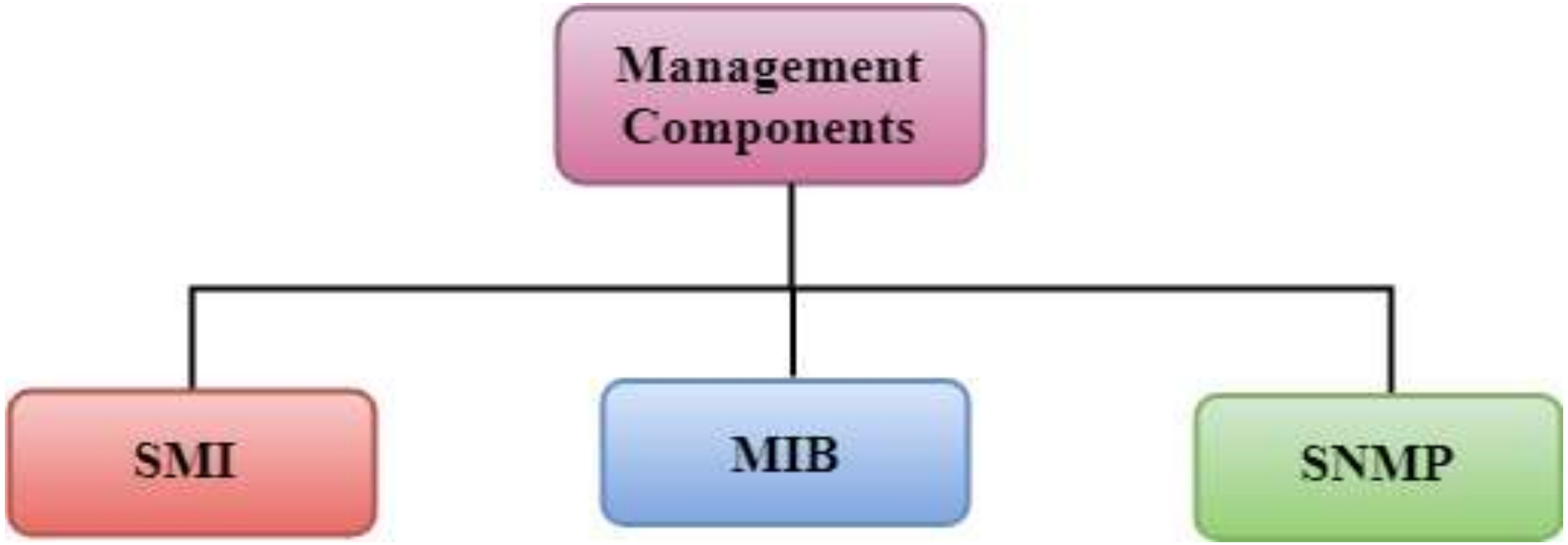


SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)

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.

SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)



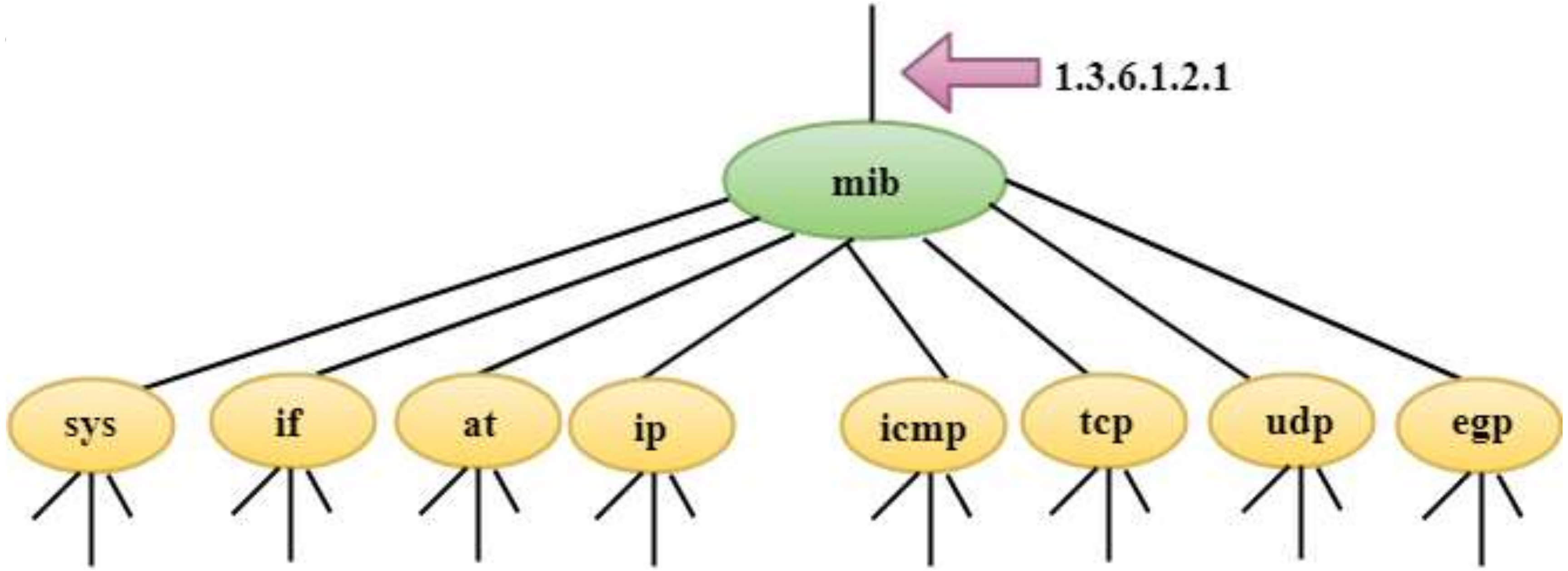
SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)

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,



SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)

SNMP

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

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.

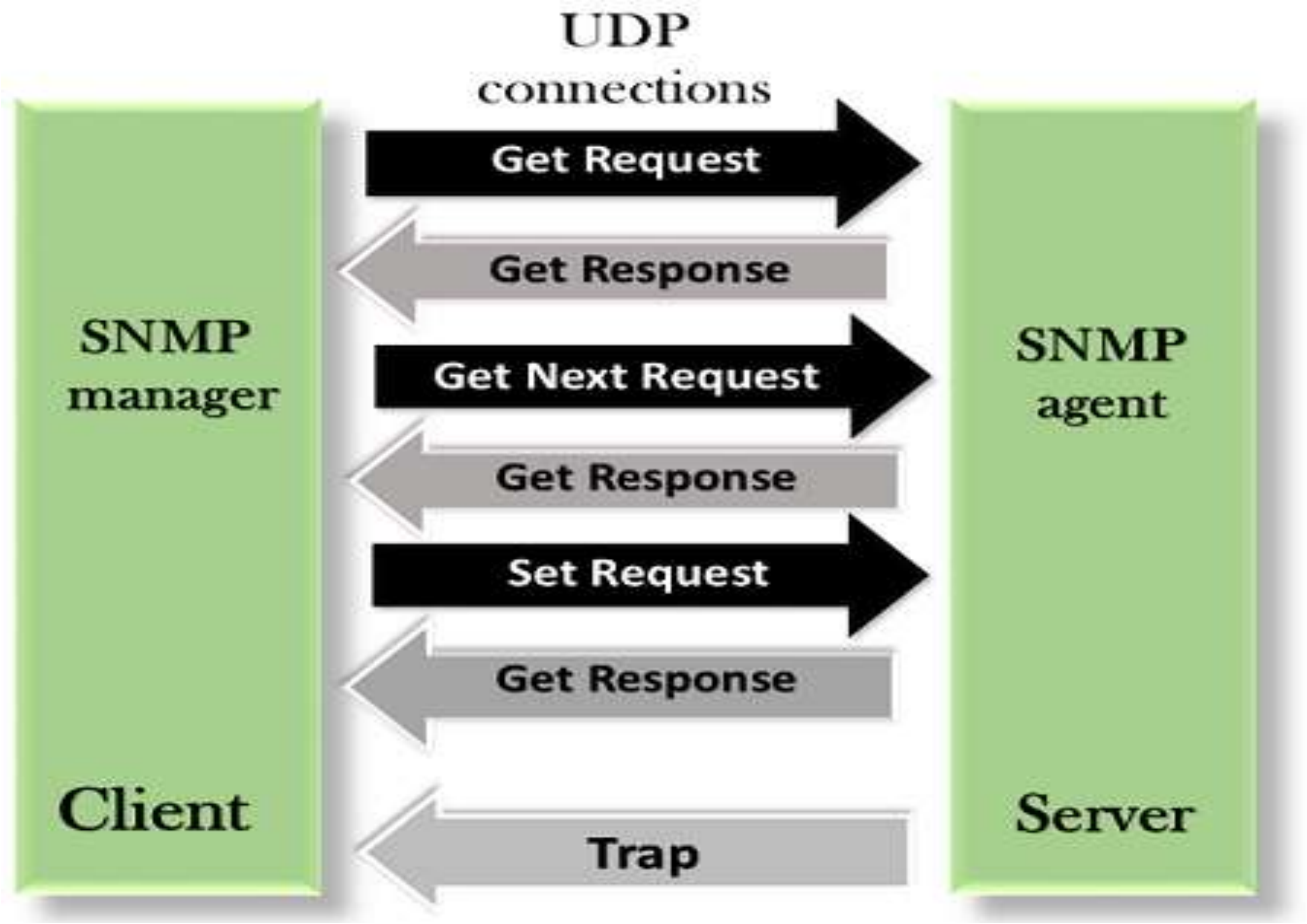
GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

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.

SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)

SNMP



FILE TRANSFER PROTOCOL (FTP)

File transfer protocol (FTP) is an Internet tool provided by TCP/IP. The first feature of FTP was developed by Abhay Bhushan in 1971. It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, and text files 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.

- It encourages the direct use of remote computers.
- It shields users from system variations (operating system, directory structures, file structures, etc.)
- It promotes the sharing of files and other types of data.

FTP Clients

FTP works on a client-server model. The FTP client is a program that runs on the user's computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection.

Some of the commands are: get the filename(retrieve the file from the directories get server), mget filename(retrieve multiple files from the server), ls(lists files available in the current directory of the server). There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

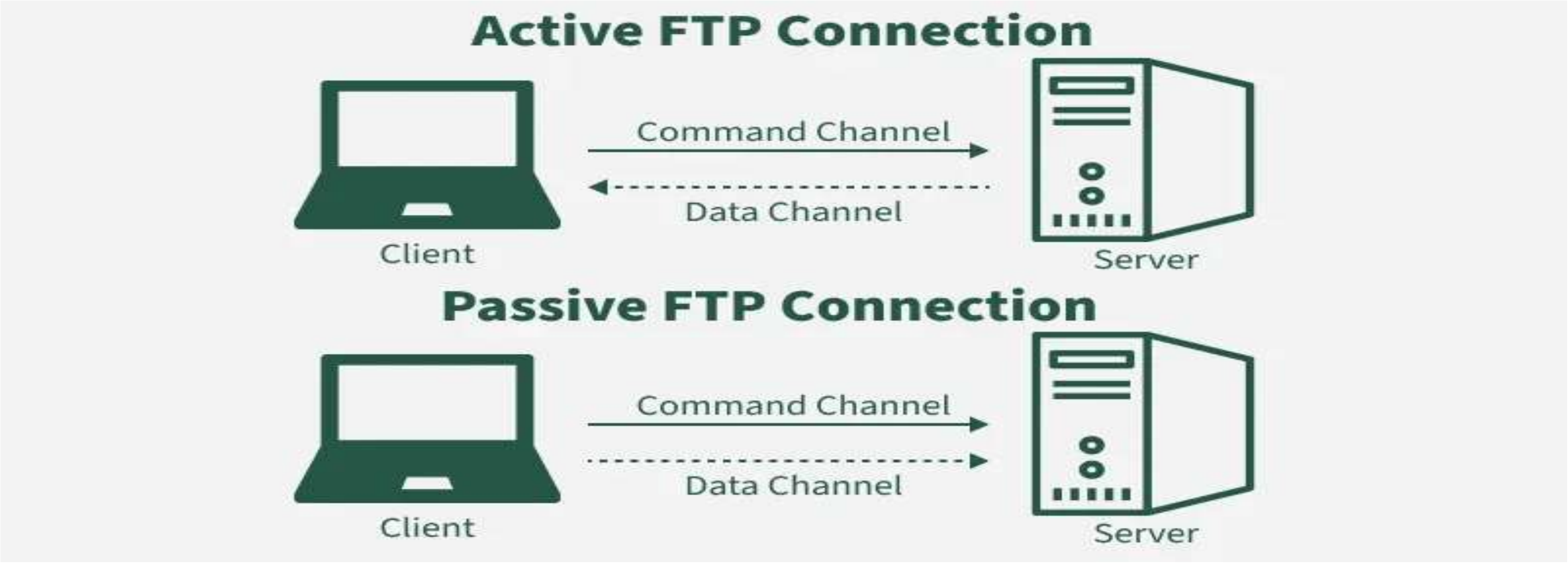
FILE TRANSFER PROTOCOL (FTP)

Type of FTP Connections

FTP connections are of two types:

1. Active FTP connection: In an Active FTP connection, the client establishes the command channel and the server establishes the data channel. When the client requests the data over the connection the server initiates the transfer of the data to the client. It is not the default connection because it may cause problems if there is a firewall in between the client and the server.

2. Passive FTP connection: In a Passive FTP connection, the client establishes both the data channel as well as the command channel. When the client requests the data over the connection, the server sends a random port number to the client, as soon as the client receives this port number it establishes the data channel. It is the default connection, as it works better even if the client is protected by the firewall.



FILE TRANSFER PROTOCOL (FTP)

Anonymous FTP

Some sites can enable anonymous FTP whose files are available for public access. So, the user can access those files without any username or password. Instead, the username is set to anonymous and the password to the guest by default. Here, the access of the user is very limited. For example, the user can copy the files but not allowed to navigate through directories.

Transmission Mode

FTP transfer files using any of the following modes:

Stream Mode: It is the default mode. In stream mode, the data is transferred from FTP to TCP in stream bytes. Here TCP is the cause for fragmenting data into small segments. The connection is automatically closed if the transforming data is in the stream bytes. Otherwise, the sender will close the connection.

Block Mode: In block mode, the data is transferred from FTP to TCP in the form of blocks, and each block followed by a 3-byte header. The first byte of the block contains the information about the block so it is known as the description block and the other two bytes contain the size of the block.

Compressed Mode: This mode is used to transfer big files. As we know that, due to the size limit we can not transfer big files on the internet, so the compressed mode is used to decrease the size of the file into small and send it on the internet.

FILE TRANSFER PROTOCOL (FTP)

Applications of FTP

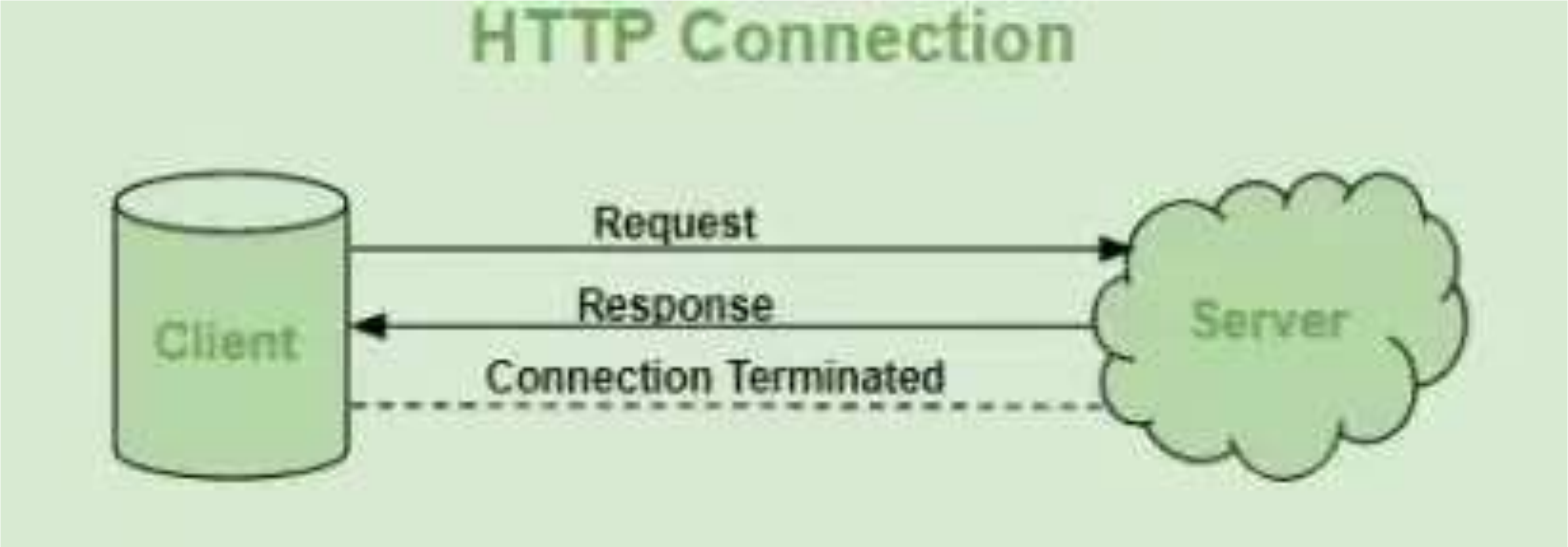
The following are the applications of FTP:

- FTP connection is used by different big business organizations for transferring files in between them, like sharing files to other employees working at different locations or different branches of the organization.
- FTP connection is used by IT companies to provide backup files at disaster recovery sites.
- Financial services use FTP connections to securely transfer financial documents to the respective company, organization, or government.
- Employees use FTP connections to share any data with their co-workers.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

HTTP (Hypertext Transfer Protocol) is a fundamental protocol of the Internet, enabling the transfer of data between a client and a server. It is the foundation of data communication for the World Wide Web.

HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.



HTTP (HYPERTEXT TRANSFER PROTOCOL)

Methods of HTTP

GET: Used to retrieve data from a specified resource. It should have no side effects and is commonly used for fetching web pages, images, etc.
POST: Used to submit data to be processed by a specified resource. It is suitable for form submissions, file uploads, and creating new resources.
PUT: Used to update or create a resource on the server. It replaces the entire resource with the data provided in the request body.
DELETE: Used to remove a specified resource from the server.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

HTTP Request/Response:

HTTP is a request-response protocol, which means that for every request sent by a client (typically a web browser), the server responds with a corresponding response. The basic flow of an HTTP request-response cycle is as follows:

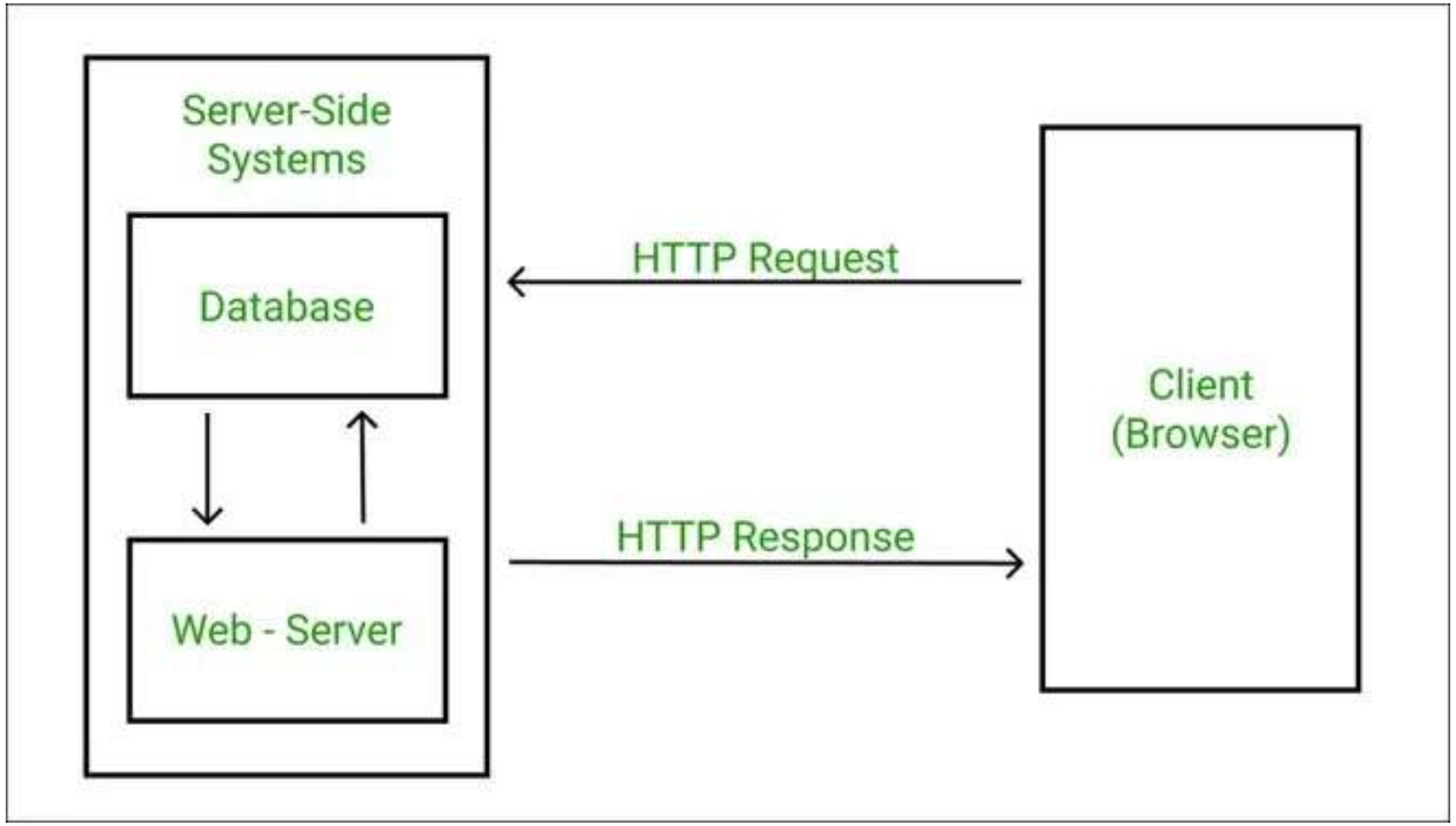
1. **Client sends an HTTP request**: The client (usually a web browser) initiates the process by sending an HTTP request to the server. This request includes a request method (GET, POST, PUT, DELETE, etc.), the target URI (Uniform Resource Identifier, e.g., a URL), headers, and an optional request body.
2. **Server processes the request**: The server receives the request and processes it based on the requested method and resource. This may involve retrieving data from a database, executing server-side scripts, or performing other operations.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

HTTP Request/Response:

3.Server sends an HTTP response: After processing the request, the server sends an HTTP response back to the client. The response includes a status code (e.g., 200 OK, 404 Not Found), response headers, and an optional response body containing the requested data or content.

4.Client processes the response: The client receives the server's response and processes it accordingly. For example, if the response contains an HTML page, the browser will render and display it. If it's an image or other media file, the browser will display or handle it appropriately.



HTTP (HYPERTEXT TRANSFER PROTOCOL)

Advantages:

- **Platform independence**: Works on any operating system
- **Compatibility**: Compatible with various protocols and technologies
- **Efficiency**: Optimized for performance
- **Security**: Supports encryption for secure data transfer

Disadvantages:

- **Lack of security**: Vulnerable to attacks like man in the middle
- **Performance issues:** Can be slow for large data transfers
- **Statelessness**: Requires additional mechanisms for maintaining state

THANK YOU