CHAPTER 5: INTERNET PROTOCOLS

Internet protocols are a set of rules that allow computers and other devices to communicate over the Internet. These protocols ensure that data is sent, received, and understood correctly between different systems. There are many types of internet protocols, each serving a specific purpose, such as transferring files, sending emails, or securing data. Understanding these protocols is important for making the internet work efficiently and securely. In this article we will see different types of internet protocol in detail.

What is the Internet Protocol?

As we discuss **Internet Protocol (IP)** is a set of rules that allows devices to communicate with each other over the Internet. It is like the address system used for sending data. Every device connected to the internet has a unique **IP address** that helps data know where to go and where it is coming from.

What is IP Addressing?

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

Working of Internet Protocol

Step by step working of internet protocol:

- **Dividing Data into Packets**: When you send information over the internet, IP split it into small parts called **packets**. Each packet contains a piece of the data and the address of where it needs to go.
- **Addressing**: Every device connected to the internet has its own **IP address**. This address helps identify where the data is being sent from and where it should be delivered.
- **Routing the Packets**: As the packets travel across the internet, they pass through several devices called **routers**. These routers help direct the packets toward the correct destination, like how mail is sorted at different post offices.
- **Reassemble the Data**: Once all the packets arrive at the destination, they are put back together to recreate the original message or file.
- **Handling Missing Packets**: If some packets don't arrive, the system can request that they be sent again, making sure the complete data is received.

This process helps data move efficiently across the internet, no matter how far it needs to travel or how many networks it passes through.

Need for Internet Protocols

The sender and receiver of data are parts of different networks, located in different parts of the world having different data transfer rates. So, we need protocols to manage the flow control of data and access control of the link being shared in the communication channel. Suppose there is a sender X who has a data transmission rate of 10 Mbps. And, there is a receiver Y who has a data receiving rate of 5Mbps. Since the rate of receiving the data is slow so some data will be lost during transmission. In order to avoid this, receiver Y needs to inform sender X about the speed mismatch so that sender X can adjust its transmission rate. Similarly, the access control decides the node which will access the link shared in the communication channel at a particular instant in time. If not the transmitted data will collide if many computers send data simultaneously through the same link resulting in the corruption or loss of data.

Understanding IP Addresses and Subnetting

IP addresses are numerical identifiers assigned to devices on a network, allowing data transmission between them, and the article delves into the purpose of IP addresses and how they are broken down.

Definition and Purpose of IP Addresses

- IP addresses are numerical identifiers assigned to devices on a network for data transmission.
- They serve as unique identifiers for devices on both local and internet networks.
- They function like street addresses for digital devices, allowing data packets to travel accurately.

IPv4 and IPv6

- The most widely used format, IPv4, uses four sets of integers from 0 to 255, whereas IPv6 uses an eight-segment alphanumeric representation that is more sophisticated and uses colons to divide the segments.
- IPv6 was developed due to concerns over IPv4 address exhaustion and features a much larger pool of available IP addresses.
- IPv6 includes additional features such as better security and support for quality-of-service traffic shaping.

How IP Addresses are Broken Down?

- The host section identifies a particular device within that network, whereas the network portion identifies the network to which the device belongs.
- The host section identifies a particular device within that network, whereas the network portion identifies the network to which the device belongs.
- IPv4 addressing uses dotted decimal notation, while IPv6 addressing uses a similar breakdown with considerably more digits per section.

Differences Between IPv4 and IPv6

- The main difference between them is the number of bits used to define an IP address: IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses.

- IPv6 includes additional features and a vast increase in available IP addresses, making it superior to IPv4 in many ways.
- IPv4 still remains in use today alongside IPv6 due to backward compatibility issues and slow adoption by some service providers.

Comprehensive Guide to IP Subnetting

The comprehensive guide to IP subnetting includes a step-by-step breakdown, practice problems and examples, and even provides a subnetting calculator for easy subnet creation.

Step-by-Step Guide to Subnetting

Subnetting can be complex, but with the proper guidance, it can become a simple process. Here's a step-by-step guide to subnetting?

- Determine the number of subnets required by your network.
- Identify the block size for the subnets you need.
- Choose an appropriate IP address range for the subnet.
- Write out the binary representation of the chosen IP address range.
- Decide on the number of bits to use in the subnet mask for each subnet.
- Convert these bits into decimal notation to get your subnet mask.
- Calculate your available host addresses per subnet by subtracting two from your total address space (one for network ID and one for broadcast).
- Assign IP addresses to devices on each subnet, starting with assigning a unique network ID and broadcast address.

Following these steps will make subnetting easier and manageable, allowing efficient management of your network resources and better control over traffic flow optimization.

IP Address Table and Resource Guide

The IP Address Table and Resource Guide includes important information on IP address formats, subnet mask notations, CIDR notation, and a subnetting cheat sheet for managing subnets.

IP Address Formats and Subnet Mask Notations

One of the critical aspects of understanding IP addresses and subnetting is knowing the different IP address formats and subnet mask notations. This knowledge allows for more manageable and accurate network configurations. The following HTML table summarizes the variations in IP address formats and subnet mask notations, providing a quick reference guide for better clarity.

IP Version	Address Format	Subnet Mask Format	Example
IPv4	Decimal Notation	Decimal Notation	192.168.1.1 / 255.255.255.0
IPv4	Decimal Notation	CIDR Notation	192.168.1.1 /24

IPv6	Hexadecimal Notation	Decimal Notation	2001:0db8:85a3:0000:0000:8a2e:0370:7334 / 64
IPv6	Hexadecimal Notation	CIDR Notation	2001:0db8:85a3::8a2e:0370:7334 /64

This table covers the primary IP address formats (decimal and hexadecimal notations) and subnet mask notations (decimal and CIDR notations) for both IPv4 and IPv6. Using these formats and notations correctly can help ensure proper subnet calculations and network configurations.

CIDR Notation

CIDR notation, or Classless Inter-Domain Routing notation, is a compact way of specifying an IP address and its corresponding subnet mask. CIDR notation uses a slash (/) followed by the number of network bits to specify how many bits from the left are used for the network part of an IP address. For example, /24 indicates that the first 24 bits are allocated for the network portion of an IPv4 address.

CIDR notation is commonly used in networking to simplify addressing and routing. It allows administrators to create more efficient networks by allocating smaller blocks of addresses instead of using entire classful networks. This method conserves address space while allowing better control over routing policies and increased security through granular access controls.

In addition, CIDR notation makes it easier to represent subnets with different sizes within one major network prefix. For instance, if you have 192.168.0.x/24 and want two subnets with different numbers of hosts say 20 and 30 respectively then you could divide your remaining eight host bits into four each by using /28 (for one block), /27 (to include both blocks), allowing a total bandwidth usage that has no overlapping between them!

Subnet Mask Notation

Subnet mask notation is a way to represent the subnet mask of an IP address in a more concise and understandable manner. In this notation, the number of bits that are used for the network ID is represented by a forward slash followed by a number. For example, a subnet mask with 24 bits set to 1 (255.255.255.0) can be represented as /24.

CIDR notation uses this same format but also allows for specifying arbitrary lengths of network IDs and host IDs within an IP address range. Subnet masks are crucial for routing data between devices on different networks, so understanding how to properly use and interpret them is essential for anyone working with computer networking systems.

When configuring routers or managing subnets, it's important to have accurate information about subnet masks since they impact how traffic flows across the network. The article provides additional resources such as cheat sheets and tutorials that can help readers get comfortable with subnetting concepts quickly so they can become proficient at using these tools effectively in their work environments".

Cheat Sheet for Subnetting

Understanding IP subnetting can seem complicated, but this cheat sheet aims to simplify the process by providing a quick reference guide to subnetting. It includes pertinent information about IP address formats, subnet mask notations, and CIDR notations.

CIDR Notation	Subnet Mask	Subnet Bit	Usable Hosts
/32	255.255.255.255	0	1
/31	255.255.255.254	1	2
/30	255.255.255.252	2	4
/29	255.255.255.248	3	8
/28	255.255.255.240	4	16
/27	255.255.255.224	5	32
/26	255.255.255.192	6	64
/25	255.255.255.128	7	128
/24	255.255.255.0	8	256

This table provides a quick reference for converting CIDR notations to subnet masks, determining the number of subnet bits, and calculating the number of usable hosts. As you progress through the comprehensive guide on IP subnetting, this cheat sheet will serve as a helpful tool to better understand the concepts and calculations involved in subnetting.

Types of Internet Protocol

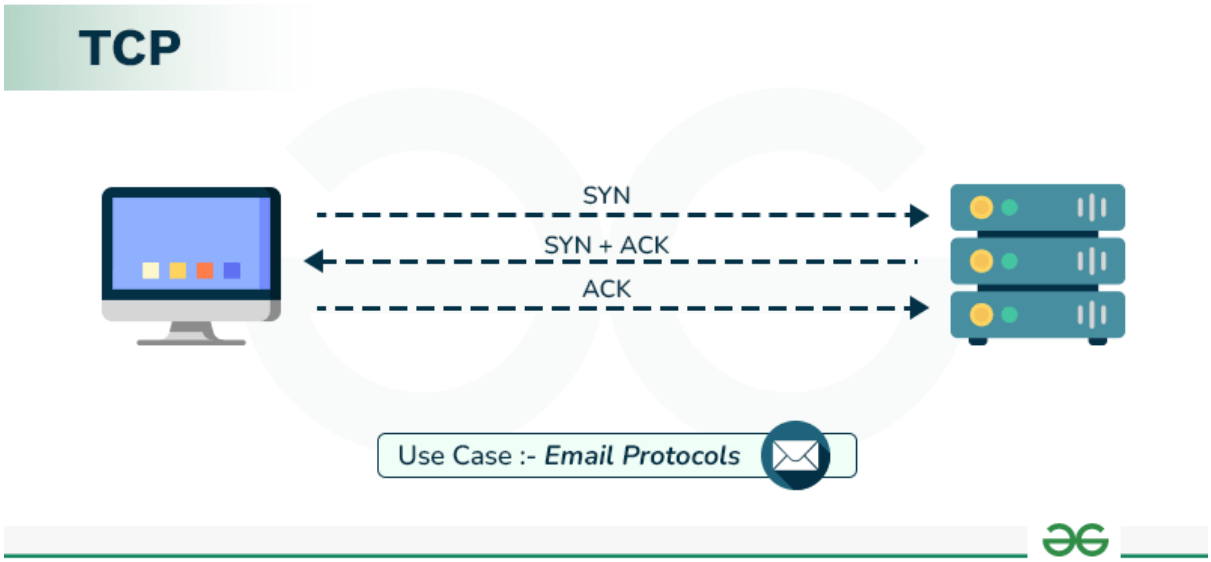
Internet Protocols are of different types having different uses. These are mentioned below:

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)
2. SMTP(Simple Mail Transfer Protocol)
3. PPP(Point-to-Point Protocol)
4. FTP (File Transfer Protocol)
5. SFTP(Secure File Transfer Protocol)
6. HTTP(Hyper Text Transfer Protocol)
7. HTTPS(HyperText Transfer Protocol Secure)
8. TELNET(Terminal Network)
9. POP3(Post Office Protocol 3)
10. IPv4
11. IPv6
12. ICMP
13. UDP
14. IMAP

15. SSH

1. TCP/IP (Transmission Control Protocol/ Internet Protocol)

In TCP/IP, the IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination. The TCP is also known as a connection-oriented protocol.

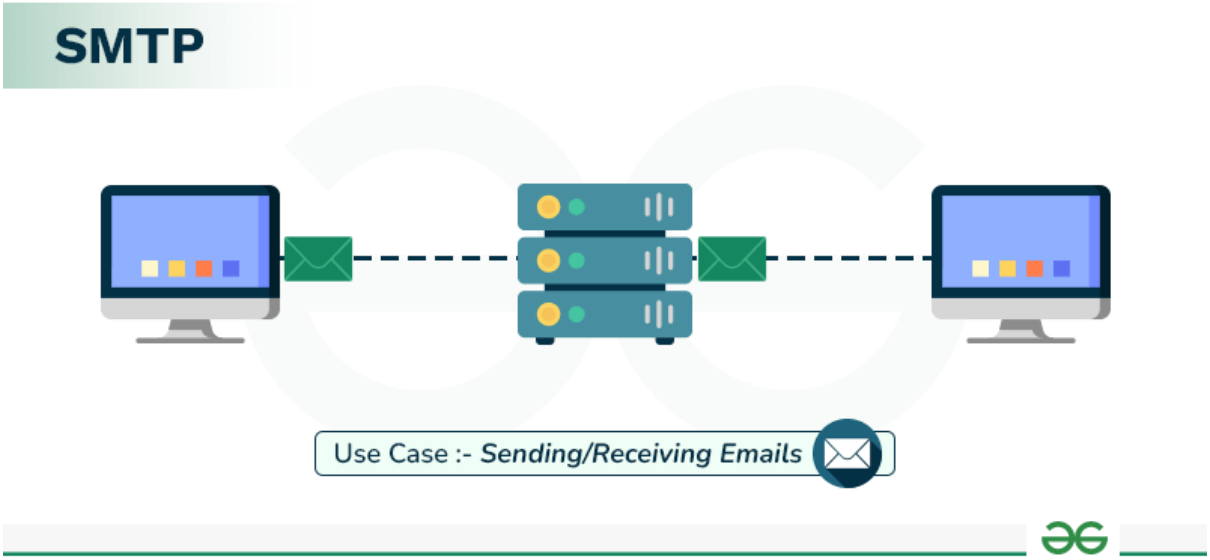


TCP/IP

For more details, please refer TCP/IP Model article.

2. SMTP(Simple Mail Transfer Protocol)

SMTP protocol is important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mail. And as soon as it delivers the mail to the receiving email id, it removes the email from the outgoing list. The message or the electronic mail may consider the text, video, image, etc. It helps in setting up some communication server rules.



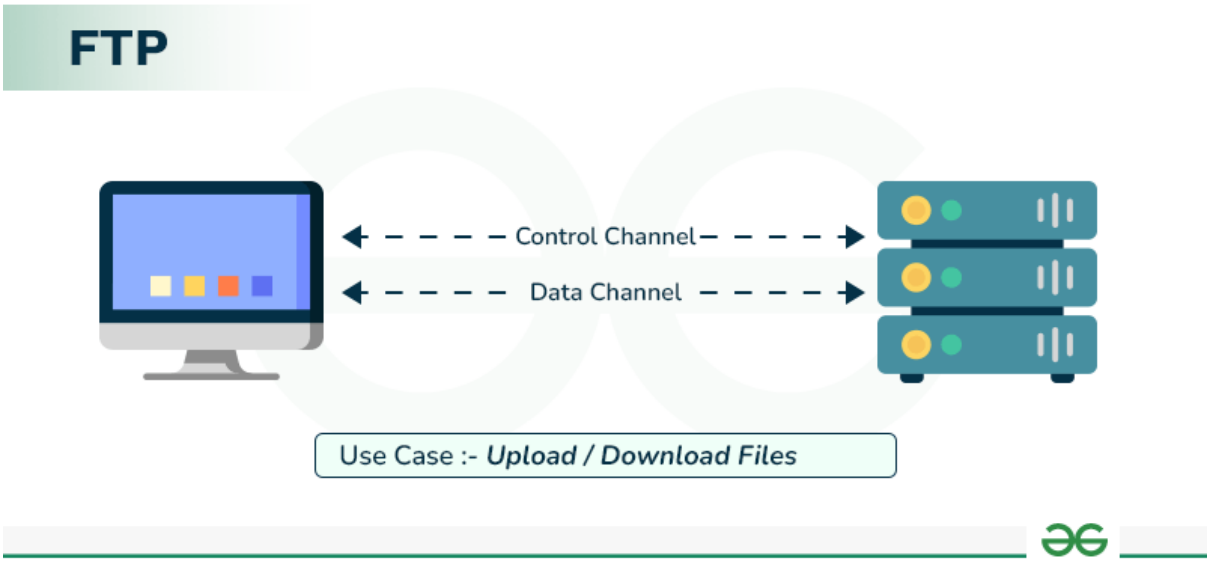
SMTP

3. PPP (Point-to-Point Protocol)

PPP is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate with each other and exchange information with each other. For example, A user connects his PC to the server of an Internet Service Provider and also uses PPP. Similarly, for connecting two routers for direct communication it uses PPP.

4. FTP (File Transfer Protocol)

This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates each other using their ID and Password. And, the desired file transfer takes place between the machines.



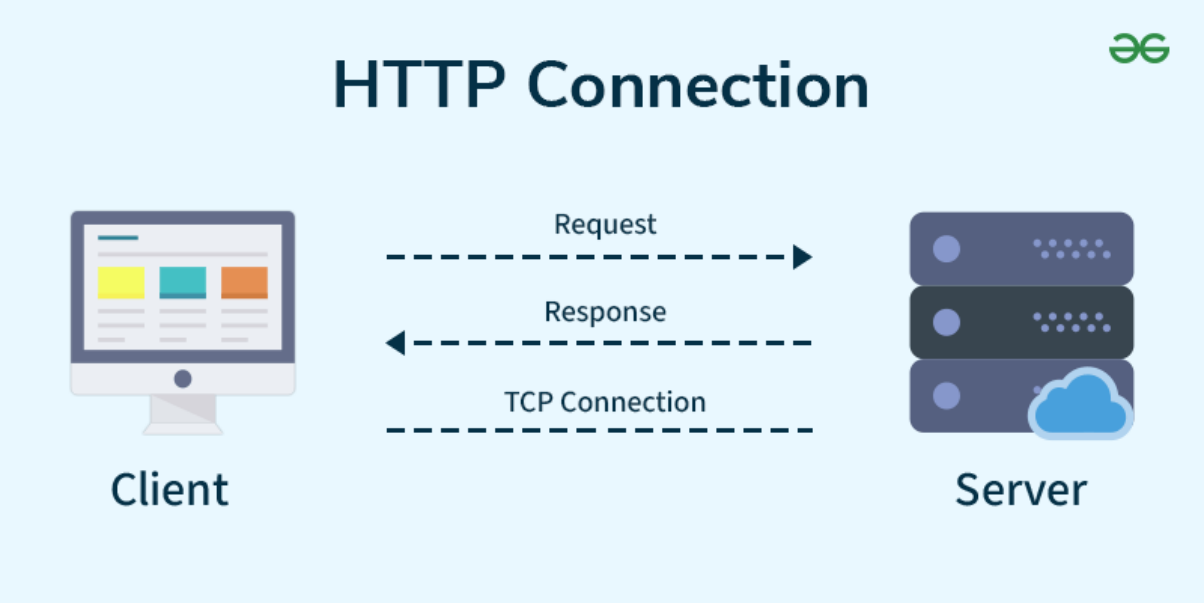
FTP

5. SFTP(Secure File Transfer Protocol)

SFTP which is also known as SSH FTP refers to File Transfer Protocol (FTP) over Secure Shell (SSH) as it encrypts both commands and data while in transmission. SFTP acts as an extension to SSH and encrypts files and data then sends them over a secure shell data stream. This protocol is used to remotely connect to other systems while executing commands from the command line.

6. HTTP(Hyper Text Transfer Protocol)

HTTP protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol that is being used to share text, images, and other multimedia files on the World Wide Web.



HTTP

7. HTTPS (HyperText Transfer Protocol Secure)

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network with the SSL/TLS protocol for encryption and authentication. So, generally, a website has an HTTP protocol but if the website is such that it receives some sensitive information such as credit card details, debit card details, OTP, etc then it requires an SSL certificate installed to make the website more secure. So, before entering any sensitive information on a website, we should check if the link is HTTPS or not. If it is not HTTPS then it may not be secure enough to enter sensitive information.

8. TELNET (Terminal Network)

TELNET is a standard TCP/IP protocol used for virtual terminal service given by ISO. This enables one local machine to connect with another. The computer which is being connected is called a remote computer and which is connecting is called the local computer. TELNET operation lets us display anything being performed on the remote computer in the local computer. This operates on the

client/server principle. The local computer uses the telnet client program whereas the remote computer uses the telnet server program.

9. POP3(Post Office Protocol 3)

POP3 stands for Post Office Protocol version 3. It has two Message Access Agents (MAAs) where one is client MAA (Message Access Agent) and another is server MAA(Message Access Agent) for accessing the messages from the mailbox. This protocol helps us to retrieve and manage emails from the mailbox on the receiver mail server to the receiver's computer. This is implied between the receiver and the receiver mail server. It can also be called a one-way client-server protocol. The POP3 works on two ports i.e port 110 and port 995.

10. IPv4

The fourth and initially widely used version of the Internet Protocol is called IPv4 (Internet Protocol version 4). It is the most popular version of the Internet Protocol and is in charge of distributing data packets throughout the network. Maximum unique addresses for IPv4 are 4,294,967,296 (232), which are possible due to the use of 32-bit addresses. The network address and the host address are the two components of each address. The host address identifies a particular device within the network, whereas the network address identifies the network to which the host belongs. In the "dotted decimal" notation, which is the standard for IPv4 addresses, each octet (8 bits) of the address is represented by its decimal value and separated by a dot (e.g. 192.168.1.1).

11. IPv6

The most recent version of the Internet Protocol, IPv6, was created to address the IPv4 protocol's drawbacks. A maximum of 4.3 billion unique addresses is possible with IPv4's 32-bit addresses. Contrarily, IPv6 uses 128-bit addresses, which enable a significantly greater number of unique addresses. This is significant because IPv4 addresses were running out and there are an increasing number of devices that require internet access. Additionally, IPv6 offers enhanced security features like integrated authentication and encryption as well as better support for mobile devices. IPv6 support has spread among websites and internet service providers, and it is anticipated to gradually displace IPv4 as the main internet protocol.

For more details, please refer Differences between IPv4 and IPv6 article.

12. ICMP

ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information about network conditions. It is an integral part of the Internet Protocol (IP) suite and is used to help diagnose and troubleshoot issues with network connectivity. ICMP messages are typically generated by network devices, such as routers, in response to errors or exceptional conditions encountered in forwarding a datagram. Some examples of ICMP messages include:

- Echo Request and Echo Reply (ping)
- Destination Unreachable
- Time Exceeded
- Redirect

ICMP can also be used by network management tools to test the reachability of a host and measure the round-trip time for packets to travel from the source to the destination and back. It should be noted that ICMP is not a secure protocol, it can be used in some types of network attacks like DDoS amplification.

13. UDP

UDP (User Datagram Protocol) is a connectionless, unreliable transport layer protocol. Unlike TCP, it does not establish a reliable connection between devices before transmitting data, and it does not guarantee that data packets will be received in the order they were sent or that they will be received at all. Instead, UDP simply sends packets of data to a destination without any error checking or flow control. UDP is typically used for real-time applications such as streaming video and audio, online gaming, and VoIP (Voice over Internet Protocol) where a small amount of lost data is acceptable and low latency is important. UDP is faster than TCP because it has less overhead. It doesn't need to establish a connection, so it can send data packets immediately. It also doesn't need to wait for confirmation that the data was received before sending more, so it can transmit data at a higher rate.

14. IMAP

IMAP (Internet Message Access Protocol) is a protocol used for retrieving emails from a mail server. It allows users to access and manage their emails on the server, rather than downloading them to a local device. This means that the user can access their emails from multiple devices and the emails will be synced across all devices. IMAP is more flexible than POP3 (Post Office Protocol version 3) as it allows users to access and organize their emails on the server, and also allows multiple users to access the same mailbox.

15. SSH

SSH (Secure Shell) is a protocol used for secure remote login and other secure network services. It provides a secure and encrypted way to remotely access and manage servers, network devices, and other computer systems. SSH uses public-key cryptography to authenticate the user and encrypt the data being transmitted, making it much more secure than traditional remote login protocols such as Telnet. SSH also allows for secure file transfers using the SCP (Secure Copy) and SFTP (Secure File Transfer Protocol) protocols. It is widely used in Unix-based operating systems and is also available for Windows. It is commonly used by system administrators, developers, and other technical users to remotely access and manage servers and other network devices.

CHAPTER 6: NETWORK PROTOCOLS

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the **Open Systems Interface (OSI) model** proposed by ISO.

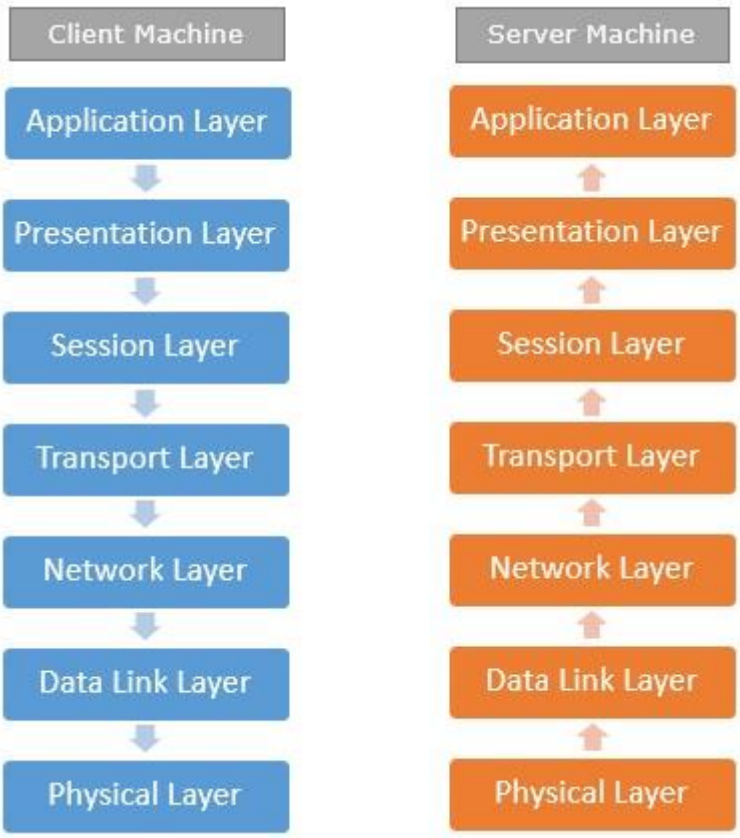
OSI Model

OSI model is not a **network architecture** because it does not specify the exact services and protocols for each layer. It simply tells what each layer should do by defining its input and output data. It is up to network architects to implement the layers according to their needs and resources available.

These are the seven layers of the OSI model −

- **Physical layer** −It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Cards hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.
- **Data link layer** − It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
- **Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.
- **Transport layer** − Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.
- **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data.

- **Presentation layer** – This layer is concerned with correct representation of data, i.e. syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.
- **Application layer** – It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.



It is not necessary for every network to have all the layers. For example, network layer is not there in broadcast networks.

When a system wants to share data with another workstation or send a request over the network, it is received by the application layer. Data then proceeds to lower layers after processing till it reaches the physical layer.

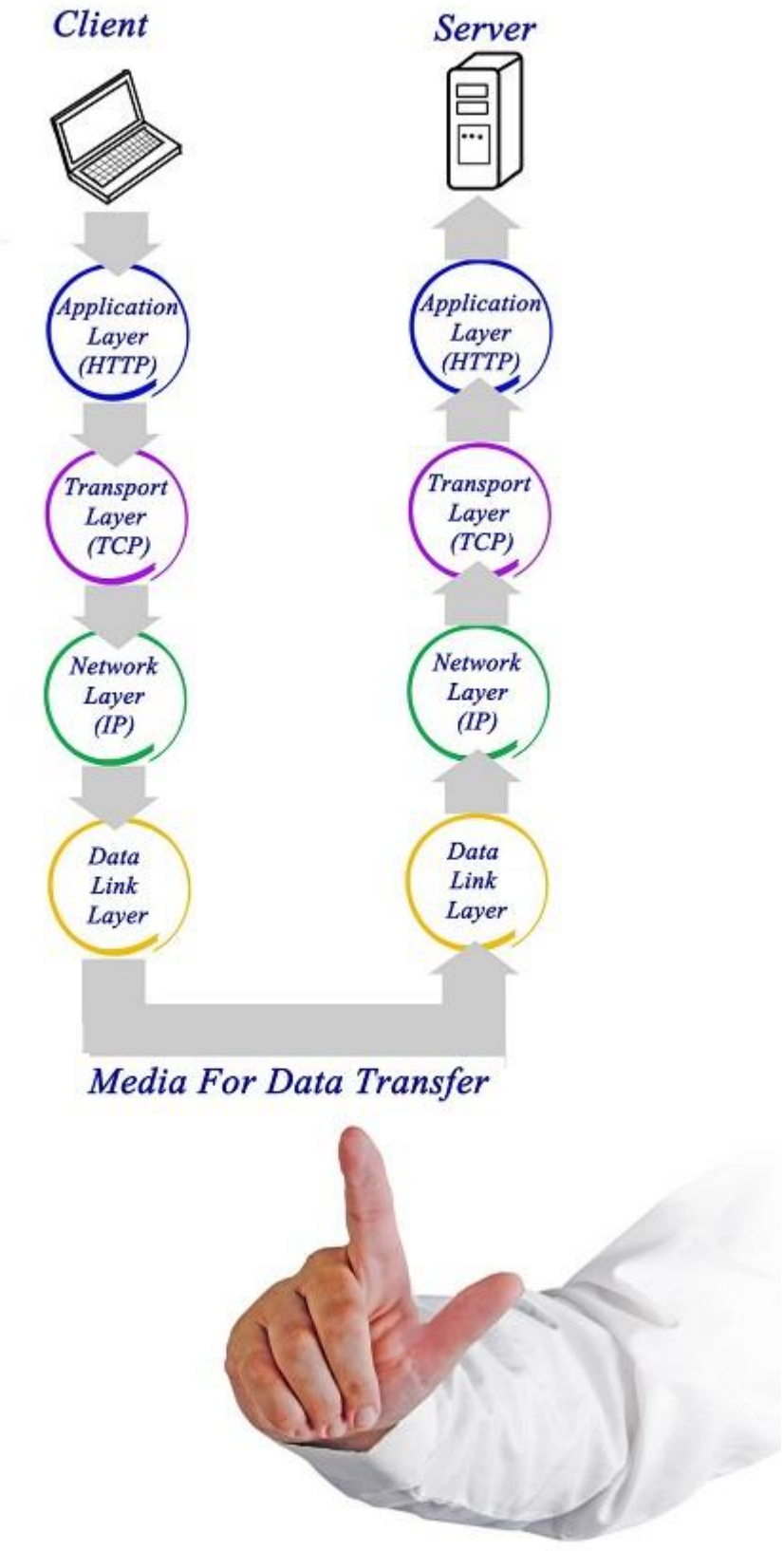
At the physical layer, the data is actually transferred and received by the physical layer of the destination workstation. There, the data proceeds to upper layers after processing till it reaches application layer.

At the application layer, data or request is shared with the workstation. So each layer has opposite functions for source and destination workstations. For example, data link layer of the source workstation adds start and stop flags to the frames but the same layer of the destination workstation will remove the start and stop flags from the frames.

Let us now see some of the protocols used by different layers to accomplish user requests.

TCP/IP

TCP/IP stands for **Transmission Control Protocol/Internet Protocol**. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model. A computer that sends a request is the client and a computer to which the request is sent is the server.



TCP/IP has four layers −

- **Application layer** − Application layer protocols like HTTP and FTP are used.

- **Transport layer** − Data is transmitted in form of datagrams using the Transmission Control Protocol (TCP). TCP is responsible for breaking up data at the client side and then reassembling it on the server side.
- **Network layer** − Network layer connection is established using Internet Protocol (IP) at the network layer. Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.
- **Data link layer** − Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.

TCP/IP is widely used in many communication networks other than the Internet.

FTP

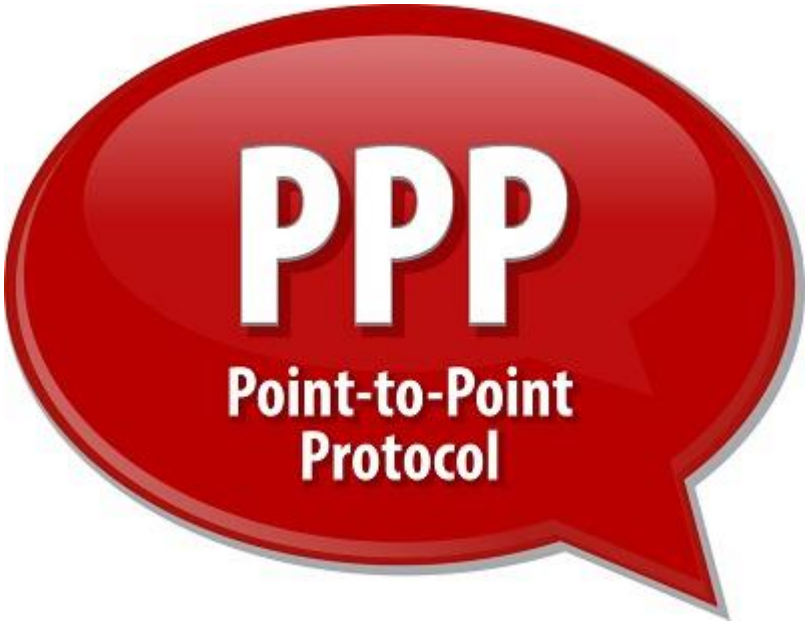
As we have seen, the need for network came up primarily to facilitate sharing of files between researchers. And to this day, file transfer remains one of the most used facilities.The protocol that handles these requests is **File Transfer Protocol** or **FTP**.

Using FTP to transfer files is helpful in these ways −

- Easily transfers files between two different networks
- Can resume file transfer sessions even if connection is dropped, if protocol is configure appropriately
- Enables collaboration between geographically separated teams

PPP

Point to Point Protocol or PPP is a data link layer protocol that enables transmission of TCP/IP traffic over serial connection, like telephone line.



To do this, PPP defines these three things −

- A framing method to clearly define end of one frame and start of another, incorporating errors detection as well.
- Link control protocol (LCP) for bringing communication lines up, authenticating and bringing them down when no longer needed.
- Network control protocol (NCP) for each network layer protocol supported by other networks.

Using PPP, home users can avail Internet connection over telephone lines.