**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 Card’s 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.

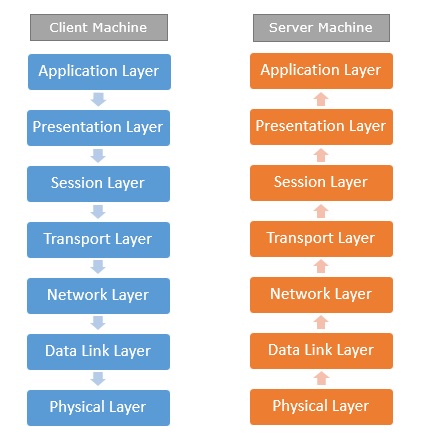
**Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.

**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.

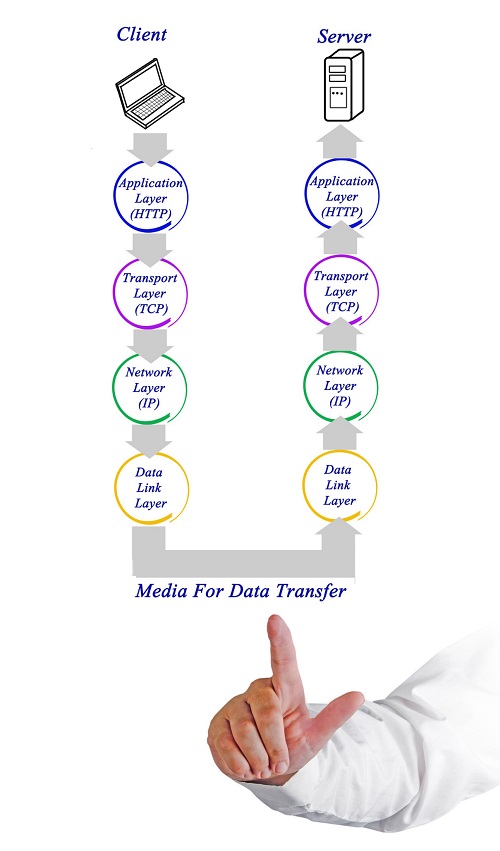
At the physical layer, the data is actually transferred and received by the physical layer of the destination workstation. There, the data proceeds to upper layers after processing till it reaches application layer.

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.

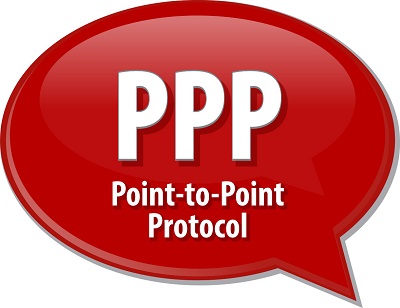


Using FTP to transfer files is helpful in these ways −

* 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.

**HTTP**

The hypertext transfer protocol, abbreviated HTTP, is a system by which computers talk to each other across the World Wide Web. It's used by computers and smart phones to ask web servers to send the contents of websites and to submit data through online forms. HTTP is text-based, and it's designed to be readable by humans as well as machines.

## Purpose of HTTP Protocol

The name hypertext transfer protocol refers to HTTP's role in transmitting website data across the internet. Hypertext refers to the standard form of websites in which one page can refer users to another page through clickable hyperlinks, usually simply called links. The purpose of the HTTP protocol is to provide a standard way for web browsers and servers to talk to each other.

**Simple Mail Transfer Protocol (SMTP)**

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver’s side.

**SMTP Fundamentals**   
SMTP is an application layer protocol. 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 always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

**SMTP Protocol**

The SMTP model is of two type :

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination’s host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver’s SMTP. 

The client SMTP is the one which initiates the session let us call it as the client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

# **Remote login**

One of the initial motivations for building computer networks was to allow users to access remote computers over the networks. In the 1960s and 1970s, the mainframes and the emerging minicomputers were composed of a central unit and a set of terminals connected through serial lines or modems. The simplest protocol that was designed to access remote computers over a network is probably [telnet](https://www.computer-networking.info/2nd/html/glossary.html" \l "term-telnet) [RFC 854](https://tools.ietf.org/html/rfc854.html). [telnet](https://www.computer-networking.info/2nd/html/glossary.html" \l "term-telnet) runs over TCP and a telnet server listens on port 23 by default. The TCP connection used by telnet is bidirectional, both the client and the server can send data over it. The data exchanged over such a connection is essentially the characters that are typed by the user on the client machine and the text output of the processes running on the server machine with a few exceptions (e.g. control characters, characters to control the terminal like VT-100, ...) . The default character set for telnet is the ASCII character set, but the extensions specified in [RFC 5198](https://tools.ietf.org/html/rfc5198.html) support the utilisation of Unicode characters.

From a security viewpoint, the main drawback of [telnet](https://www.computer-networking.info/2nd/html/glossary.html" \l "term-telnet) is that all the information, including the usernames, passwords and commands, is sent in cleartext over a TCP connection. This implies that an eavesdropper could easily capture the passwords used by anyone on an unprotected network. Various software tools exist to automate this collection of information. For this reason, [telnet](https://www.computer-networking.info/2nd/html/glossary.html" \l "term-telnet) is rarely used today to access remote computers. It is usually replaced by [ssh](https://www.computer-networking.info/2nd/html/glossary.html" \l "term-ssh) or similar protocols.

**Internet Protocol**

The Internet Protocol (IP) is the principal [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol" \o "Communications protocol) in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite" \o "Internet protocol suite) for relaying [datagrams](https://en.wikipedia.org/wiki/Datagram" \o "Datagram) across network boundaries. Its [routing](https://en.wikipedia.org/wiki/Routing" \o "Routing) function enables [internetworking](https://en.wikipedia.org/wiki/Internetworking" \o "Internetworking), and essentially establishes the [Internet](https://en.wikipedia.org/wiki/Internet" \o "Internet).

IP has the task of delivering [packets](https://en.wikipedia.org/wiki/Packet_(information_technology)" \o "Packet (information technology)) from the source [host](https://en.wikipedia.org/wiki/Host_(network)" \o "Host (network)) to the destination host solely based on the [IP addresses](https://en.wikipedia.org/wiki/IP_address" \o "IP address) in the packet [headers](https://en.wikipedia.org/wiki/Header_(computing)" \o "Header (computing)). For this purpose, IP defines packet structures that [encapsulate](https://en.wikipedia.org/wiki/Encapsulation_(networking)" \o "Encapsulation (networking)) the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the [connectionless](https://en.wikipedia.org/wiki/Connectionless_communication" \o "Connectionless communication) datagram service in the original Transmission Control Program introduced by [Vint Cerf](https://en.wikipedia.org/wiki/Vint_Cerf" \o "Vint Cerf) and [Bob Kahn](https://en.wikipedia.org/wiki/Bob_Kahn" \o "Bob Kahn) in 1974, which was complemented by a connection-oriented service that became the basis for the [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol" \o "Transmission Control Protocol) (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

**Wireless/Mobile Communication Protocol**

## GSM

GSM stands for Global System for Mobile communications. GSM is one of the most widely used digital wireless telephony system. It was developed in Europe in 1980s and is now international standard in Europe, Australia, Asia and Africa. Any GSM handset with a SIM (Subscriber Identity Module) card can be used in any country that uses this standard. Every SIM card has a unique identification number. It has memory to store applications and data like phone numbers, processor to carry out its functions and software to send and receive messages

GSM technology uses TDMA (Time Division Multiple Access) to support up to eight calls simultaneously. It also uses encryption to make the data more secure.

The frequencies used by the international standard is 900 MHz to 1800 MHz However, GSM phones used in the US use 1900 MHz frequency and hence are not compatible with the international system.

## WLL

WLL stands for Wireless in Local Loop. It is a wireless local telephone service that can be provided in homes or offices. The subscribers connect to their local exchange instead of the central exchange wirelessly. Using wireless link eliminates last mile or first mile construction of network connection, thereby reducing cost and set up time. As data is transferred over very short range, it is more secure than wired networks.

WLL system consists of user handsets and a base station. The base station is connected to the central exchange as well as an antenna. The antenna transmits to and receives calls from users through terrestrial microwave links. Each base station can support multiple handsets depending on its capacity.

## GPRS

GPRS stands for General Packet Radio Services. It is a packet based wireless communication technology that charges users based on the volume of data they send rather than the time duration for which they are using the service. This is possible because GPRS sends data over the network in packets and its throughput depends on network traffic. As traffic increases, service quality may go down due to congestion, hence it is logical to charge the users as per data volume transmitted.

GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load.