***Protocol and Its Types***

In today’s technological world, we’re talking about millions of users communicating with different devices in different languages. That also includes various ways in which they transmit data along with the software they implement. Therefore, when discussing what is protocol and its types in networking, we need to point out that communicating worldwide would not be possible if there were no fixed ‘standards’ to govern the way users communicate for data as well as the way our devices treat that data.

## What Is Protocol and Its Types in Networking?

According to the [**Florida Centre for Instructional Technology**](https://fcit.usf.edu/network/chap2/chap2.htm), protocol is defined as **a set of rules that govern the communications between computers on a network**.

[**EDUCBA**](https://www.educba.com/types-of-networking-protocols/) adds that network protocols are formalized requirements and plans consisting of **rules**, **procedures**, and **types** that describe communication among a couple of devices across the network.

In networking, protocol can be described as an approach to rules that allows entities of a communication program to transfer information through any type of variety of physical medium. The protocol “identifies the **rules**, **syntax**, **semantics**, and **synchronization of communication** and **feasible error managing methods**”.

## Types of Networking Protocols

For two computers to communicate with each other, they must be speaking the same language. Different types of network protocols and standards are required to ensure that a computer (regardless of its OS, network card, or application used) can communicate with another one located in the next room or halfway around the world.

There are seven layers of networking protocols defined by the [**OSI (Open Systems Interconnection)**](https://heimdalsecurity.com/blog/osi-layers/) Reference Model. The complexity of these layers is beyond the scope of this article, nevertheless, they were simplified below into four layers to help identify some of the protocols you should be familiar with.

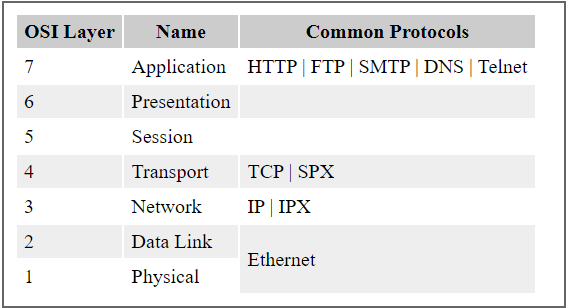


Image Source: [**Florida Centre for Instructional Technology**](https://fcit.usf.edu/network/chap2/chap2.htm)

Below, I will discuss the different types of networking protocols.

1. **Physical layer.** The [physical layer](https://www.techtarget.com/searchnetworking/definition/physical-layer) is the initial layer that physically connects two interoperable systems. It controls simplex or [duplex](https://www.techtarget.com/searchnetworking/definition/full-duplex) modem transmissions and transfers data in bits. Additionally, it oversees the hardware that connects the network interface card ([NIC](https://www.techtarget.com/searchnetworking/definition/network-interface-card)) to the network, including the wiring, cable terminators, topography and voltage levels.
2. **Data-link layer.** The [data-link layer](https://www.techtarget.com/searchnetworking/definition/Data-Link-layer) is responsible for the error-free delivery of data from one node to another over the physical layer. It's also the [firmware](https://www.techtarget.com/whatis/definition/firmware) layer of the NIC. It puts datagrams together into frames and gives each frame the start and stop flags. Additionally, it fixes issues brought on by broken, misplaced or duplicate frames.
3. **Network layer.** The [network layer](https://www.techtarget.com/searchnetworking/definition/Network-layer) is concerned with information flow regulation, switching and routing between workstations. Additionally, it divides up datagrams from the transport layer into error-free and smaller datagrams.
4. **Transport layer.** The [transport layer](https://www.techtarget.com/searchnetworking/definition/Transport-layer) transfers services from the network layer to the application layer and breaks down data into data frames for error checking at the network segment level. This also ensures that a fast host on a network doesn't overtake a slower one. Essentially, the transport layer ensures that the entire message is delivered from beginning to end. It also confirms a successful data transmission and retransmitting of the data if an error is discovered.
5. **Session layer.** The [session layer](https://www.techtarget.com/searchnetworking/definition/Session-layer) establishes a connection between two workstations that need to communicate. In addition to ensuring security, this layer oversees connection establishment, session maintenance and [authentication](https://www.techtarget.com/searchsecurity/definition/authentication).
6. **Presentation layer.** The [presentation layer](https://www.techtarget.com/searchnetworking/definition/presentation-layer) is also known as the *translation layer* because it retrieves the data from the application layer and formats it for transmission over the network. It addresses the proper representation of data, including the syntax and semantics of information. The presentation layer is also in charge of managing [file-level security](https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks) and transforming data to network standards.
7. **Application layer.** The [application layer](https://www.techtarget.com/searchnetworking/definition/Application-layer), which is the top layer of the network, oversees relaying user application requests to lower levels. File transfer, email, remote login, data entry and other common applications take place at this layer.

## Network Communication Protocols

### 1. HTTP and HTTPS

Often referred to as the protocol of the Internet, HTTP/HTTPS stands for Hypertext Transfer Protocol and Hypertext Transfer Protocol (secure) respectively.

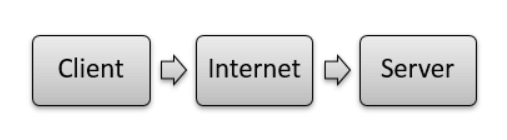


Image Source: [**EDUCBA**](https://www.educba.com/types-of-networking-protocols/)

The majority of application-layer protocols employ this model, using one device on the client’s network; the other device on the network is the server.

In the case of HTTP, Client-server principles allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

While HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, in the case of HTTPS the transferring of data is done in an encrypted format. Therefore, we can say that [**HTTPS**](https://heimdalsecurity.com/blog/https-security-101/) thwarts hackers from the interpretation or modification of data throughout the transfer of packets.

### 2. FTP (File Transfer Protocol)

FTP allows users to transfer files (program files, multimedia files, text files, documents, etc) from one machine to another.

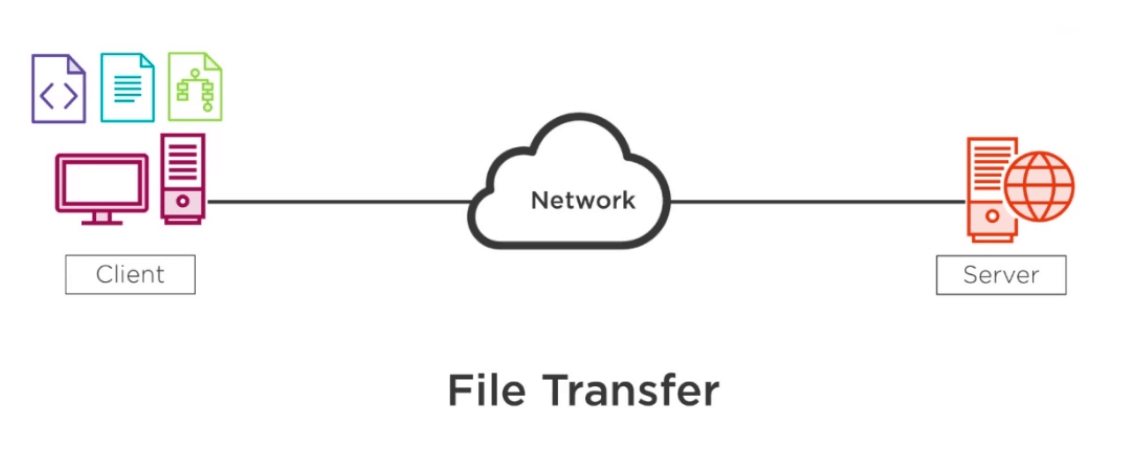


Image Source: [**EDUCBA**](https://www.educba.com/types-of-networking-protocols/)

### 3. TCP (Transmission Control Protocol)

[**TCP**](https://heimdalsecurity.com/blog/what-is-tcp/) is a popular communication protocol that separates data into packets that can be distributed across a network. Afterward, they can be sent by devices such as switches and routers to the designated targets.

### 4. UDP (User Datagram Protocol)

Although UDP works in a similar way to TCP, the main difference between the two is that TCP ensures a connection is made between the application and server, but UDP does not. User Datagram Protocol is mainly implemented for creating loss-tolerating and low-latency linking between various apps.

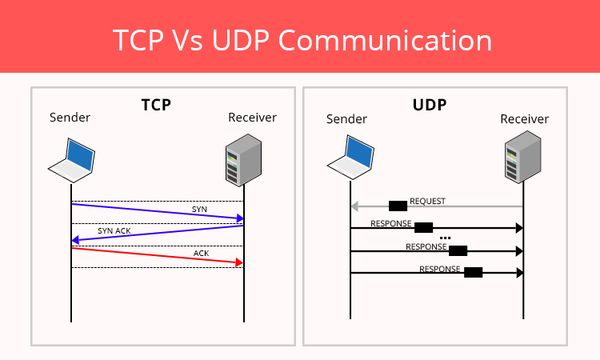


Image Source: [**CyberHoot**](https://cyberhoot.com/cybrary/transmission-control-protocol-tcp/)

### 5. IRC (Internet Relay Chat)

IRC is a text-based communication protocol that facilitates communication in the form of text. Although it supports private messages between two users, data transfer, and various server-side and client-side commands It is mainly used for group discussion in chat rooms called “channels”. This protocol works well on networks with numerous distributed machines.

## what is protocol and its types in networking IRC

Image Source: [**ResearchGate**](https://www.researchgate.net/figure/IRC-based-Botnet-Architecture-79_fig2_282477239)

## Network Management Protocols

### 1. SNMP (Simple Network Management Protocol)

[**SNMP**](https://heimdalsecurity.com/blog/what-is-snmp-in-computer-network-science/) is a standard protocol used to exchange network management information. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP provides a tool for network administrators to manage network performance, find and solve network issues, and plan for network growth.

### 2. ICMP (Internet Control Message Protocol)

ICMP is a network layer protocol mainly used to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong. It’s a protocol that believes in direct communication in the workplace.

## Network Security Protocols

### 1. SSL (Secure Socket Layer)

[**SSL**](https://heimdalsecurity.com/blog/what-is-ssl-vulnerability/) is a network security protocol used for data protection on the transport layer, and it’s located between the transport and application layer of the ISO/OSI reference model providing security services to any application-based protocols, like HTTP, FTP, LDAP, POP3. The SSL protocol is used in any client/server environment, being able to provide a series of features for the parties involved in the communication process. Data transferred with SSL is encrypted to prevent it from being readable.

### 2. SFTP (Secure File Transfer Protocol)

As its name suggests, this network security protocol is used to securely transfer files across a network. Data is encrypted and both the client and server are authenticated.

## Final Thoughts on What Is Protocol and Its Types in Networking

Every time we use the Internet, we leverage network protocols. Though you may not know how network protocols work or how frequently you encounter them, they are necessary for browsing the Internet or digital communications in any capacity.

Forging strongly into parts of existence that nobody had predicted, digital networking is additionally strengthening us for the future. New protocols and requirements will come out, new applications can be developed, and our lives will probably be further transformed and improved.

I hope this guide on what is protocol and its types in networking has been helpful. Drop a line below if you have any **comments**, **questions**, or **suggestions** related to the topic – I look forward to hearing your opinion!