# **Theory and Procedure:**

## **Command and Wireshark:**

Commands in Network are tools used in computing to interact with and manage network connections and configurations. They allow users to diagnose network issues, test connectivity, gather information about network devices, and analyze data flows. By executing these commands, users can perform tasks such as checking IP address configurations, tracing data routes, resolving domain names, and managing network protocols. These commands are especially valuable for network administrators and anyone needing to troubleshoot or optimize network performance.

These are the ones that we will be using in this project:

## **ipconfig:**

  IPCONFIG is a command-line utility windows, ReactOS, macos and collection of other Operating systems, which is used to display and manage network configuration settings such as IP addressing, subnetting mask, DNS addressing, Port identificaition, Default gateways etc.It is a global and versatile CLI used for trobuleshooting, configuting and also used to make the optimization work in connectivity.[1]

### **ping:**

this command use to verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of the corresponding echo Reply messages is displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.[2]

You can also use this command to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name isn't, you might have a name resolution problem. In this case, make sure the computer name you're specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.[2]

### **tracert:**

This command can be understood as trace root. Which tells that our computer reaches or hits which-which server for reaching the particular root.

### **nslookup:**

This command is use to transform the given searched words into their corresponding IP addresses.

### **telnet:**

allows users to establish a connection to remote devices using the Telnet protocol, often used for remote command-line access and management of servers and network devices.

### **wireshark:**

Wireshark is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.[3]

Wireshark is [cross-platform](https://en.wikipedia.org/wiki/Cross-platform), using the [Qt](https://en.wikipedia.org/wiki/Qt_(software)" \o "Qt (software)) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) in current releases to implement its user interface, and using [pcap](https://en.wikipedia.org/wiki/Pcap" \o "Pcap) to capture packets; it runs on [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS" \o "MacOS), [BSD](https://en.wikipedia.org/wiki/BSD), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), some other [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are [free software](https://en.wikipedia.org/wiki/Free_software), released under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) version 2 or any later version.[3]

## **Web Server:**

Creating a web page and server involves designing the front-end and back-end components of a web application. The front-end, built using HTML for structure, CSS for styling. The back-end, implemented using server-side technology which is java. A server hosts the web application, processes user requests, and sends responses. (The server used in this task can be any device capable of running the Server.java file). The requests which are sent by the client are HTTP request.

### **HTTP**

HTTP (Hypertext Transfer Protocol) is an [application layer](https://en.wikipedia.org/wiki/Application_layer) protocol in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite) model for distributed, collaborative, [hypermedia](https://en.wikipedia.org/wiki/Hypermedia) information systems.  HTTP is the foundation of data communication for the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web), where [hypertext](https://en.wikipedia.org/wiki/Hypertext) documents include [hyperlinks](https://en.wikipedia.org/wiki/Hyperlink) to other resources that the user can easily access, for example by a [mouse](https://en.wikipedia.org/wiki/Computer_mouse) click or by tapping the screen in a [web browser](https://en.wikipedia.org/wiki/Web_browser).[4]

### **HTML**

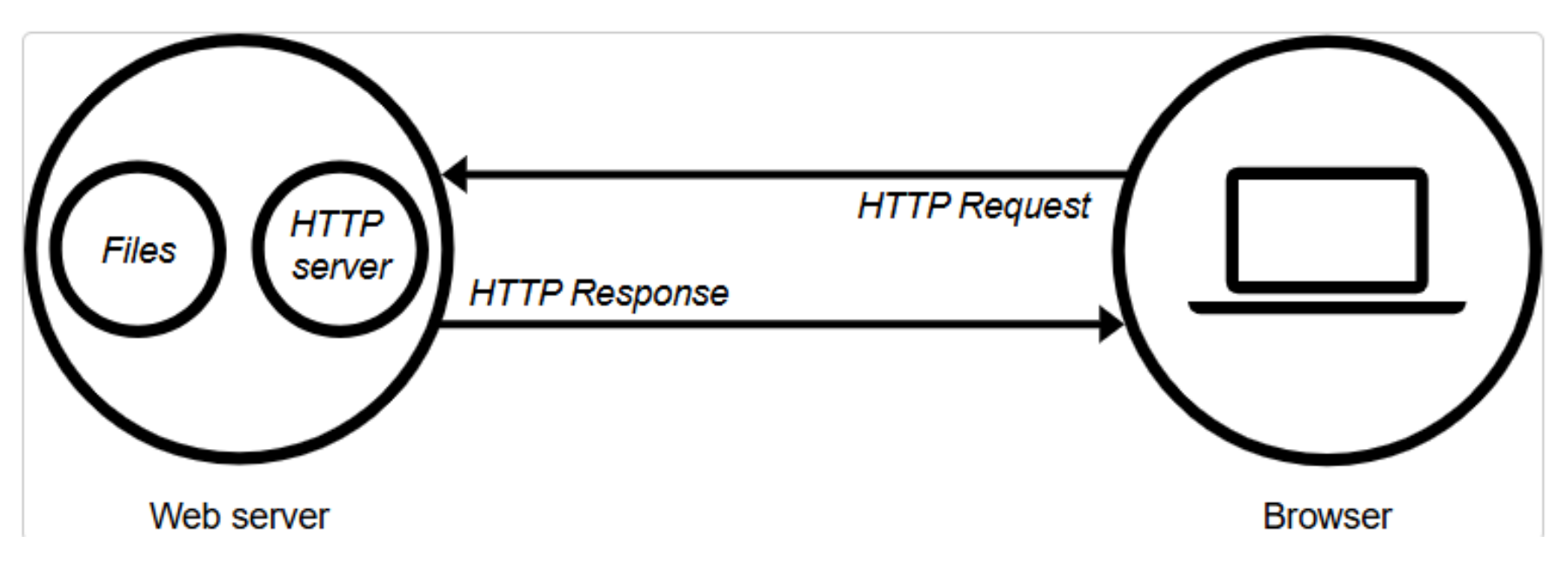
Hypertext Markup Language (HTML) is the standard [markup language](https://en.wikipedia.org/wiki/Markup_language) for documents designed to be displayed in a [web browser](https://en.wikipedia.org/wiki/Web_browser). It defines the content and structure of [web content](https://en.wikipedia.org/wiki/Web_content). It is often assisted by technologies such as [Cascading Style Sheets](https://en.wikipedia.org/wiki/Cascading_Style_Sheets) (CSS) and [scripting languages](https://en.wikipedia.org/wiki/Scripting_language) such as [JavaScript](https://en.wikipedia.org/wiki/JavaScript), a programming language.[5]

### **CSS**

(Cascading Style Sheets) is a style sheet language used to control the appearance and layout of HTML elements on a webpage. It allows developers to apply styles such as colors, fonts, spacing, and animations, creating visually appealing and responsive designs. By separating content (HTML) from presentation (CSS), it makes websites easier to maintain and adapt for different devices.

### **Java**

is a powerful programming language often used for backend development to build dynamic, secure, and scalable web applications. It supports server-side operations, such as processing user requests, managing databases, and generating dynamic web pages. Frameworks like Spring and Hibernate enhance Java’s capabilities, making it a preferred choice for creating robust backend systems for enterprise-level applications.



### **HTTP responses**

HTTP responses can vary depending on the client’s request. In this task, we are specifically focused on serving the following types of content:

* HTML pages
* CSS stylesheets
* Images (JPG or PNG)
* Video files (MP4)

These types of files make up the content that is displayed in the user's browser when accessing a webpage

**How Web Servers Work:**

1. **Client Request**: The process begins when a client (usually a browser) sends an HTTP request to the server, specifying the resource it wants (e.g., /index.html).

2. **Server Processing:** The web server processes the request by:

* Locating the requested resource in its storage.
* Executing server-side logic if the request involves dynamic content (e.g., using PHP or Python scripts).

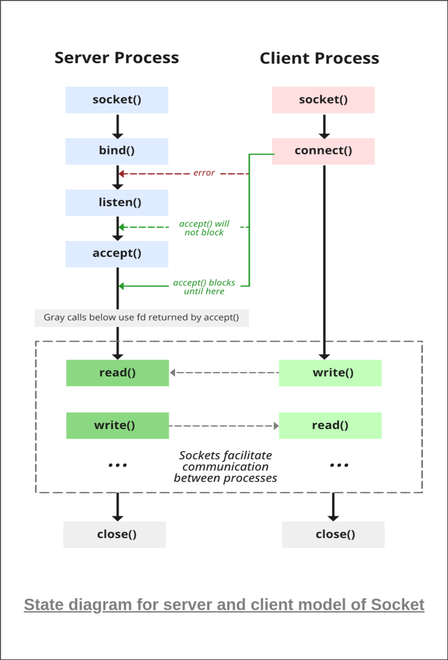
3. **Server Response:** The server sends an HTTP response back to the client, which includes:

* Status Code: Indicates the result of the request (e.g., 200 OK, 404 Not Found).
* Headers: Provide metadata about the response (e.g., Content-Type: text/html).
* Body: Contains the actual content (e.g., an HTML page or JSON data).

4. **Client Rendering:** The client processes the response and displays it to the user.

## **Socket Programming:**

In addition, the purpose of Task 3 is to develop a game using Socket Programming, aiming to provide a clear understanding of how communication occurs between a UDP server and its clients through sockets. The server is responsible for sending and receiving messages via sockets, while clients perform similar actions to exchange data with the server. This setup illustrates the concept of real-time communication over a network. Moreover, threads are employed to handle multiple clients simultaneously, ensuring synchronization and coordination between the server and all connected clients. This approach highlights the importance of managing concurrent connections effectively and demonstrates how threads enable seamless and synchronized interactions in a multi-client environment.

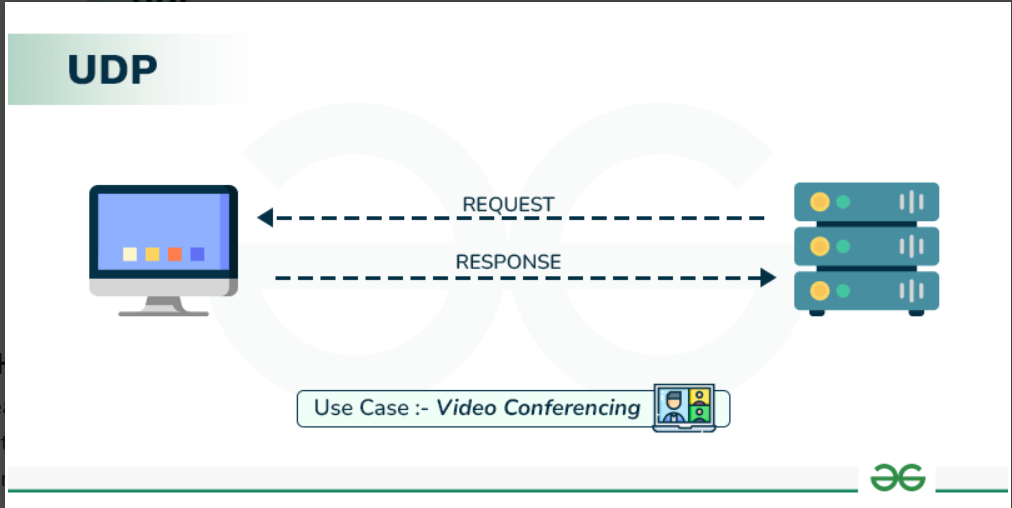


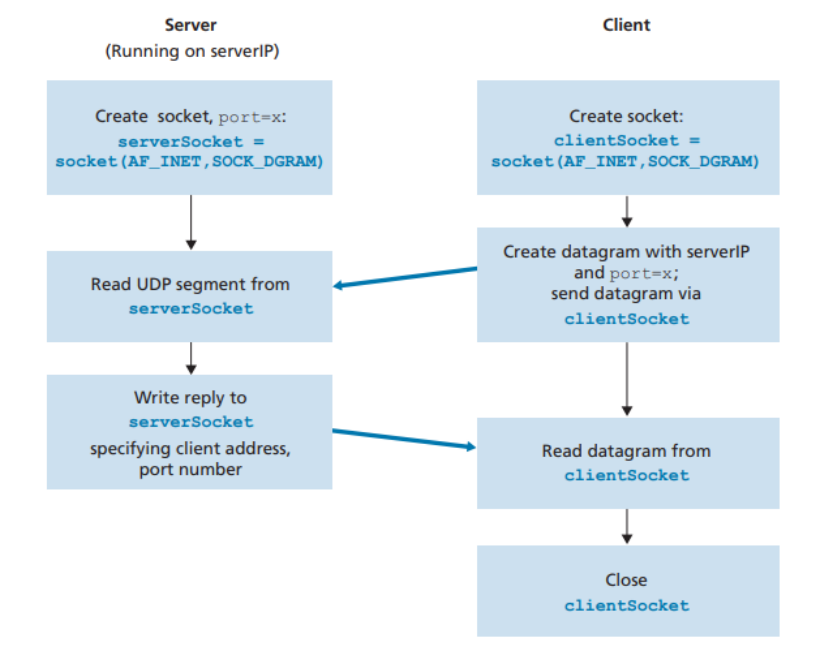
## **UDP and TCP connection**

### **UDP Connection:**

**User Datagram Protocol (UDP)**is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.**So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections over the network. The UDP enables process-to-process communication.[6]

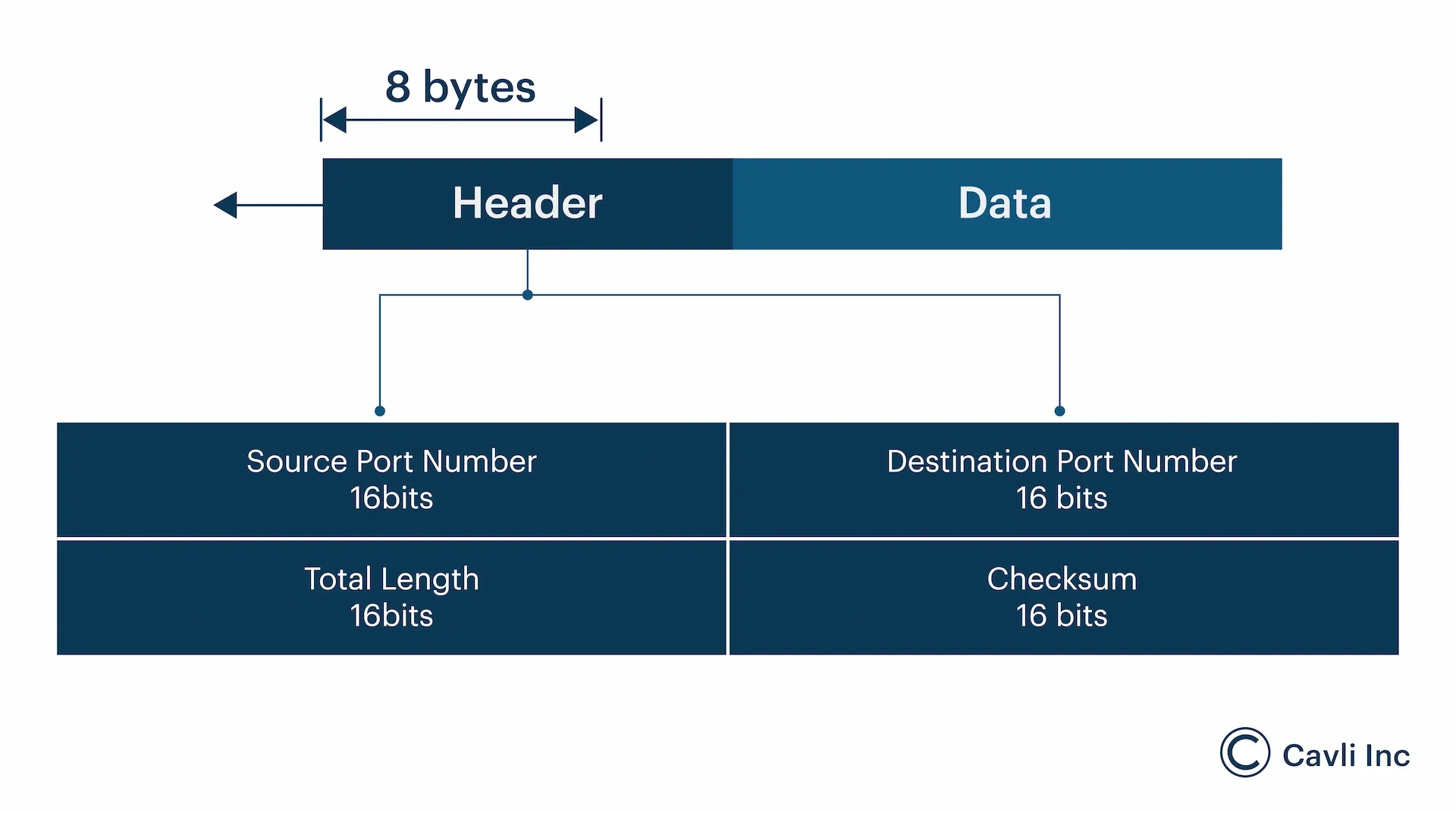
User Datagram Protocol (UDP) is one of the core protocols of the Internet Protocol (IP) suite. It is a communication protocol used across the internet for time-sensitive transmissions such as video playback or [DNS lookups](https://www.geeksforgeeks.org/dns-look-up/). Unlike Transmission Control Protocol (TCP), UDP is connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.[6]





### **UDP Header:**

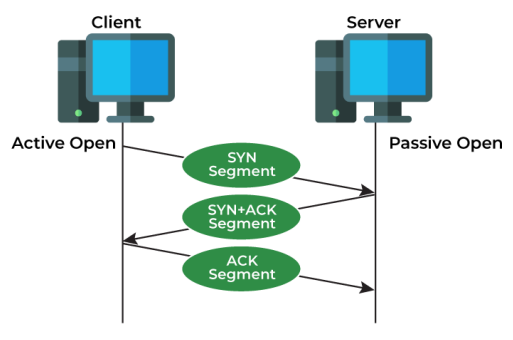
UDP header is an 8-byte fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.

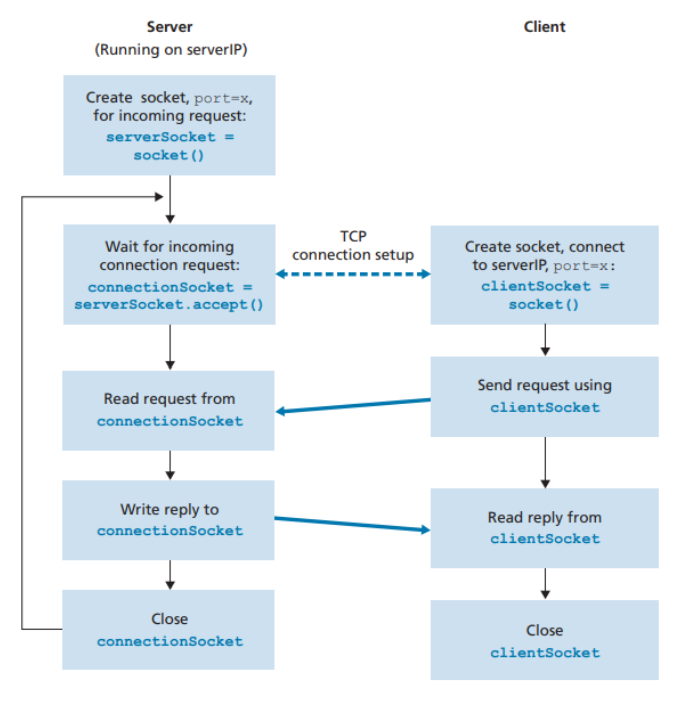


### **TCP Connection:**

The Transmission Control Protocol (TCP) is one of the main [protocols](https://en.wikipedia.org/wiki/Communications_protocol) of the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). It originated in the initial network implementation in which it complemented the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP). Therefore, the entire suite is commonly referred to as [TCP/IP](https://en.wikipedia.org/wiki/TCP/IP). TCP provides [reliable](https://en.wikipedia.org/wiki/Reliability_(computer_networking)), ordered, and [error-checked](https://en.wikipedia.org/wiki/Error_detection_and_correction) delivery of a [stream](https://en.wikipedia.org/wiki/Reliable_byte_stream) of [octets](https://en.wikipedia.org/wiki/Octet_(computing)) (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web), email, [remote administration](https://en.wikipedia.org/wiki/Remote_administration), and [file transfer](https://en.wikipedia.org/wiki/File_transfer) rely on TCP, which is part of the [transport layer](https://en.wikipedia.org/wiki/Transport_layer) of the TCP/IP suite. [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) often runs on top of TCP.[7]

TCP is [connection-oriented](https://en.wikipedia.org/wiki/Connection-oriented_communication), meaning that sender and receiver firstly need to establish a connection based on agreed parameters; they do this through three-way handshake procedure. The server must be listening (passive open) for connection requests from clients before a connection is established. Three-way [handshake](https://en.wikipedia.org/wiki/Handshake_(computing)) (active open), [retransmission](https://en.wikipedia.org/wiki/Retransmission_(data_networks)), and error detection adds to reliability but lengthens [latency](https://en.wikipedia.org/wiki/Network_latency). Applications that do not require reliable [data stream](https://en.wikipedia.org/wiki/Data_stream) service may use the [User Datagram Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP) instead, which provides a [connectionless](https://en.wikipedia.org/wiki/Connectionless_communication) [datagram](https://en.wikipedia.org/wiki/Datagram) service that prioritizes time over reliability. TCP employs [network congestion avoidance](https://en.wikipedia.org/wiki/TCP_congestion_control). However, there are vulnerabilities in TCP, including [denial of service](https://en.wikipedia.org/wiki/Denial-of-service_attack), [connection hijacking](https://en.wikipedia.org/wiki/TCP_sequence_prediction_attack), TCP veto, and [reset attack](https://en.wikipedia.org/wiki/TCP_reset_attack).[7]





The primary difference between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) lies in their approach to connections. TCP is a connection-oriented protocol, ensuring reliable data transfer but at a slower speed. In contrast, UDP is connectionless, offering faster data transmission with less reliability. These characteristics make each protocol better suited for specific types of data transfers based on the need for speed or reliability.

Ref:

[1] <https://www.geeksforgeeks.org/ipconfig-full-form/>

[2] <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ping>

[3] <https://en.wikipedia.org/wiki/Wireshark>

[4] <https://en.wikipedia.org/wiki/HTTP>

[5] <https://en.wikipedia.org/wiki/HTML>

[6] <https://www.geeksforgeeks.org/user-datagram-protocol-udp/>

[7] <https://en.wikipedia.org/wiki/Transmission_Control_Protocol>