RESEARCH AND DEVELOPMENT DOCUMENT

**ON**

**Working of TCP & UDP Protocols & Working of HTTP, HTTPS and ICMP Protocol**

A blue background with white text

AI-generated content may be incorrect.

A blue background with white text

AI-generated content may be incorrect.

By

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

Under

Celebal Summer Internship on Cloud Infra & Security

Table of Contents

[Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) 3](#_Toc198899094)

Transmission Control Protocol (TCP) ……………………………………………………………………………………..3

User Datagram Protocol (UDP)……………………………………………………………………………………………….[4](#_Toc198899099)

[Hypertext Transfer Protocol (HTTP)…………………………..…………………………………………………………..8](#_Toc198899101)

[Hypertext Transfer Protocol Secure(HTTPS) 9](#_Toc198899102)

[Internet Control Message Protocol (ICMP)……………………………………………………………….. 10](#_Toc198899103)

References…………………………………………………………………………………………………………………………13

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) both are protocols of the Transport Layer Protocols. TCP is a connection-oriented protocol whereas UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. In this article, we will discuss the differences between TCP and UDP.

**Transmission Control Protocol (TCP)**

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

get updates separately.

**Features of TCP**

* TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
* Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
* TCP implements an error control mechanism for reliable data transfer.
* TCP considers the level of congestion in the network.

**Applications of TCP**

* **World Wide Web (WWW)**: When you browse websites, TCP ensures reliable data transfer between your browser and web servers.
* **Email**: TCP is used for sending and receiving emails. Protocols like **SMTP**(Simple Mail Transfer Protocol) handle email delivery across servers.
* **File Transfer Protocol (FTP)**: FTP relies on TCP to transfer large files securely. Whether you’re uploading or downloading files, TCP ensures data integrity.
* **Secure Shell (SSH)**: SSH sessions, commonly used for remote administration, rely on TCP for encrypted communication between client and server.
* **Streaming Media**: Services like Netflix, YouTube, and Spotify use TCP to stream videos and music. It ensures smooth playback by managing data segments and retransmissions.

**Advantages of TCP**

* It is reliable for maintaining a connection between Sender and Receiver.
* It is responsible for sending data in a particular sequence.
* Its operations are not dependent on Operating System.
* It allows and supports many routing protocols.
* It can reduce the speed of data based on the speed of the receiver.

**Disadvantages of TCP**

* It is slower than UDP and it takes more bandwidth.
* Slower upon starting of transfer of a file.
* It does not have a multicast or broadcast category.
* It does not load the whole page if a single data of the page is missing.

**User Datagram Protocol (UDP)**

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the 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 establish over the network. The UDP enables process-to-process communication.

**Features of UDP**

* Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
* It is a suitable protocol for multicasting as UDP supports packet switching.
* UDP is used for some routing update protocols like RIP (Routing Information Protocol) .
* Normally used for real-time applications which cannot tolerate uneven delays between sections of a received message.

**Application of UDP**

* Real-Time Multimedia Streaming: UDP is ideal for streaming audio and video content. Its low-latency nature ensures smooth playback, even if occasional data loss occurs.
* Online Gaming: Many online games rely on UDP for fast communication between players.
* DNS (Domain Name System) Queries: When your device looks up domain names (like converting “www.example.com” to an IP address), UDP handles these requests efficiently.
* Network Monitoring: Tools that monitor network performance often use UDP for lightweight, rapid data exchange.
* Multicasting: UDP supports packet switching, making it suitable for multicasting scenarios where data needs to be sent to multiple recipients simultaneously.
* Routing Update Protocols: Some routing protocols, like RIP (Routing Information Protocol), utilize UDP for exchanging routing information among routers.

**Advantages of UDP**

* It does not require any connection for sending or receiving data.
* Broadcast and Multicast are available in UDP.
* UDP can operate on a large range of networks.
* UDP has live and real-time data.
* UDP can deliver data if all the components of the data are not complete.

**Disadvantages of UDP**

* We cannot have any way to acknowledge the successful transfer of data.
* UDP cannot have the mechanism to track the sequence of data.
* UDP is connectionless, and due to this, it is unreliable to transfer data.
* In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
* UDP can drop packets in case of detection of errors.

**Differences between TCP and UDP**

|  |  |
| --- | --- |
| **Transmission Control Protocol (TCP)** | **User Datagram Protocol (UDP)** |
| **Transmission Control Protocol is a connection-oriented protocol.** | **User Datagram Protocol is a connectionless protocol.** |
| **As a message makes its way across the internet from one computer to another. This is connection based.** | **UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.** |
| TCP is suited for applications that require high reliability, and transmission time is relatively less critical. | **UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.** |
| The speed for TCP is slower than UDP. | UDP is faster because error recovery is not attempted. It is a "best effort" protocol. |
| TCP header size is 20 bytes | UDP Header size is 8 bytes. |
| Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries. | Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent. |
| TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control. | UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP. |
| SYN, SYN-ACK, ACK | No handshake (connectionless protocol) |

**Working of TCP and UDP**

A TCP connection is established via a three-way handshake, which is a process of initiating and acknowledging a connection. Once the connection is established data transfer can begin. After transmission, the connection is terminated by closing of all established virtual circuits.

UDP uses a simple transmission model without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service, and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Unlike TCP, UDP is compatible with packet broadcasts (sending to all on local network) and multicasting (send to all subscribers).

**Hypertext Transfer Protocol (HTTP)**

HTTP is an application-layer protocol used for transmitting hypermedia documents, such as HTML. It is the foundation of data communication on the World Wide Web. HTTP is an Application Layer Protocol ,it works on the top of the TCP/IP stack.

**Key Features:**

* **Stateless:** Each request-response pair is independent.
* **Client-Server Model:** Clients (browsers) send requests; servers respond with resources.
* **Text-Based:** Messages are in plain text, making them human-readable.

**Working Mechanism:**

1. **Client Request:**
   * The client sends an HTTP request to the server, specifying the desired resource.
2. **Server Response:**
   * The server processes the request and returns an HTTP response, which includes a status code and the requested content.

**Common HTTP Methods:**

* **GET:** Retrieve data from the server.
* **POST:** Submit data to the server.
* **PUT:** Update existing data.
* **DELETE:** Remove data.

**Working of HTTP:**

1. You Type a URL
2. DNS Resolves Domain Name
3. TCP Connection Established
4. Browser Sends HTTP Request
5. Server Sends HTTP Response

**HTTP Status Codes**

* 1xx (Informational): Request received, continuing process.
* 2xx (Success): The action was successfully received, understood, and accepted.
  + 200 OK: The request has succeeded.
* 3xx (Redirection): Further action needs to be taken to complete the request.
  + 301 Moved Permanently: The resource has been moved to a new URL.
* 4xx (Client Error): The request contains bad syntax or cannot be fulfilled.
  + 404 Not Found: The server has not found anything matching the Request-URI.
* 5xx (Server Error): The server failed to fulfil an apparently valid request.
  + 500 Internal Server Error: The server encountered an unexpected condition.

**Hypertext Transfer Protocol Secure (HTTPS)**

HTTPS stands for Hypertext Transfer Protocol Secure. It is the most common protocol for sending data between a web browser and a website. HTTPS is the secure variant of HTTP and is used to communicate between the user's browser and the website, ensuring that data transfer is encrypted for added security.

Any website, especially those requiring login details, should use HTTPS. You can see a padlock icon in the URL bar, which means the page is secure. Browsers, like Google Chrome, treat HTTPS seriously and mark non-HTTPS websites as "Not Secure."

**Working of HTTPS**

HTTPS establishes the communication between the browser and the web server. It uses the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocol for establishing communication. The new version of SSL is TLS (Transport Layer Security).

HTTPS uses the conventional HTTP protocol and adds a layer of SSL/TLS over it. The workflow of HTTP and HTTPS remains the same, the browsers and servers still communicate with each other using the HTTP protocol. However, this is done over a secure SSL connection. The SSL connection is responsible for the encryption and decryption of the data that is being exchanged to ensure data safety.

**Advantage of HTTPS**

* Secure Communication: HTTPS establishes a secure communication link between the communicating system by providing encryption during transmission.
* Data Integrity: By encrypting the data, HTTPS ensures data integrity. This implies that even if the data is compromised at any point, the hackers won't be able to read or modify the data being exchanged.
* Privacy and Security: HTTPS prevents attackers from accessing the data being exchanged passively, thereby protecting the privacy and security of the users.
* Faster Performance: TTPS encrypts the data and reduces its size. Smaller size accounts for faster data transmission in the case of HTTPS.

**Internet Control Message Protocol (ICMP)**

Internet Control Message Protocol is known as ICMP. The protocol is at the network layer. It is mostly utilized on network equipment like routers and is utilized for error handling at the network layer. Since there are various kinds of network layer faults, ICMP can be utilized to report and troubleshoot these errors.

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol (ICMP) to provide error control.

**Uses of ICMP**

ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any message which is large enough for the receiver, in that case, the receiver will drop the message and reply to the ICMP message to the source.

Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility.

* Traceroute: Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.
* Ping: Ping is a simple kind of traceroute known as the echo-request message, it is used to measure the time taken by data to reach the destination and return to the source, these replies are known as echo-replies to messages.

**Working of ICMP**

* The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake.
* ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data. ICMP datagram is like a packet, which is an independent data entity.

**Advantages of ICMP**

* Network devices use ICMP to send error messages, and administrators can use the Ping and Tracert commands to debug the network.
* These alerts are used by administrators to identify issues with network connectivity.
* A prime example is when a destination or gateway host notifies the source host via an ICMP message if there is a problem or a change in network connectivity that needs to be reported. Examples include when a destination host or networking becomes unavailable, when a packet is lost during transmission, etc.
* Furthermore, network performance and connection monitoring tools commonly employ ICMP to identify the existence of issues that the network team has to resolve.
* One quick and simple method to test connections and find the source is to use the ICMP protocol, which consists of queries and answers.

**Disadvantages of ICMP**

* If the router drops a packet, it may be due to an error; but, because to the way the IP (internet protocol) is designed, there is no way for the sender to be notified of this problem.
* Assume, while a data packet is being transmitted over the internet, that its lifetime is over and that the value of the time to live field has dropped to zero. In this case, the data packet is destroyed.
* Although devices frequently need to interact with one another, there isn't a standard method for them to do so in Internet Protocol. For instance, the host needs to verify the destination's vital signs to see if it is still operational before transmitting data.

**References**

* Geeks For Geeks
* Diffen.com
* YouTube