**Protocol:**

A communication protocol is a system of rules that allows two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.

Types of Protocols:

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. Post office Protocol (POP) Simple mail transport Protocol (SMTP) File Transfer Protocol (FTP) Hyper Text Transfer Protocol (HTTP)

**Protocols for each layer of OSI Model.:**

|  |  |  |
| --- | --- | --- |
| **Layer** | **Name** | **Protocols** |
| Layer 7 | Application | SMTP, HTTP, FTP, POP3, SNMP |
| Layer 6 | Presentation | MPEG, ASCH, SSL, TLS |
| Layer 5 | Session | NetBIOS, SAP |
| Layer 4 | Transport | TCP, UDP |
| Layer 3 | Network | IPV6, ICMP |
| Layer 2 | Data Link | ATM, Fiber Cable, etc. |
| Layer 1 | Physical | RS232 |

**IPsec:**

The IP security (IPsec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets

IPsec is a framework of related protocols that secure communications at the network or packet processing layer. It can be used to protect one or more data flows between peers. IPsec enables data confidentiality, integrity, origin authentication and anti-replay.

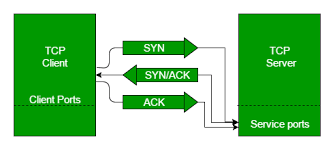
The three main IPsec protocols: **IPsec Authentication Header (AH), IPsec Encapsulating Security Payload (ESP)**, and **the IPsec Internet Key Exchange (IKE)**. for both IPv4 and IPv6 networks, and operation in both versions is similar.

**difference between TCP and UDP:**

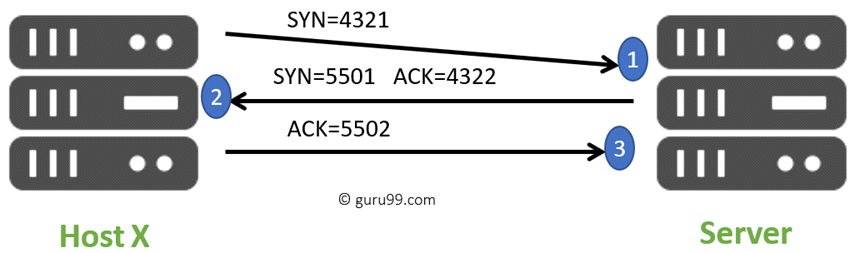
|  |  |
| --- | --- |
| **TCP** | **UDP** |
| TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data. | UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission. |
| TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgement of data. | UDP has only the basic error checking mechanism using checksums. |
| Acknowledgement segment is present. | No acknowledgement segment. |
| Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| TCP is heavy-weight. | UDP is lightweight. |
| Uses handshakes such as SYN, ACK, SYN-ACK | It’s a connectionless protocol i.e. No handshake |
| TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |
| TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet. | UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP. |

**3-way handshake:**

A three-way handshake is also known as a TCP handshake or SYN-SYN-ACK, and requires both the client and server to exchange SYN (synchronization) and ACK (acknowledgment) packets before actual data communication begins.



**scenario for 3-way handshake. Explain with the help of diagram:**



Here is a simple example of the three-way handshake process that is consists of three steps:

* Host X begins the connection by sending the TCP SYN packet to its host destination. The packets contain a random sequence number (For example, 4321) that indicates the beginning of the sequence numbers for data that the Host X should transmit.
* After that, the Server will receive the packet, and it responds with its sequence number. It’s response also includes the acknowledgment number, that is Host X’s sequence number incremented with 1 (Here, it is 4322).
* Host X responds to the Server by sending the acknowledgment number that is mostly server’s sequence number that is incremented by 1.

After the data transmission process is over, TCP automatically terminates the connection between two separate endpoints.

## Summary

* TCP 3-way handshake or three-way handshake or TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between server and client.
* Syn use to initiate and establish a connection
* ACK helps to confirm to the other side that it has received the SYN.
* SYN-ACK is a SYN message from local device and ACK of the earlier packet.
* FIN is used for terminating a connection.
* TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server
* In the first step, the client establishes a connection with a server
* In this second step, the server responds to the client request with SYN-ACK signal set
* In this final step, the client acknowledges the response of the Server
* TCP automatically terminates the connection between two separate endpoints.

**How TCP Syn Attack can be performed:**

SYN flood attacks work by exploiting the handshake process of a TCP connection. Under normal conditions, TCP connection exhibits three distinct processes in order to make a connection. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

SYN floods are a form of DDoS attack that attempts to flood a system with requests in order to consume resources and ultimately disable it. You can prevent SYN flood attacks by installing an IPS, configuring your firewall, installing up to date networking equipment, and installing commercial monitoring tools.

**TCP and UDP Examples:**

TCP:

World Wide Web(HTTP)

E-mail (SMTP TCP)

File Transfer Protocol (FTP)

Secure Shell (SSH)

UDP:

Domain Name System (DNS)

Streaming media applications such as movies

Online multiplayer games

Voice over IP (VoIP)

Trivial File Transfer Protocol (TFTP)

**TCP** is used mostly among the devices to establish a connection among the server saying it to be LAN. Searching in google. Etc.

Whereas UDP is used with creating sockets, ports and mostly in video streaming as it is much fast then tcp.