TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. TCP is defined by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards document number 793.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection(OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Session Layer.

TCP Protocol stands for Transmission Control Protocol. It is a connection oriented and reliable protocol. Connection oriented mean the connection remains established until the message has been exchanged and after the complete exchange of packet the connection is terminated. It has been put under the Transport layer. It is responsible for breaking of data messages in to packets that are sent by using internet protocol. TCP is also used in remote login i.e. one can get access of the other computer for maintenance or trouble shooting purposes. It is also used in file transfers.

TCP provides the following facilities:-

1. It groups the bytes in TCP segments and then passes them to IP.

2. With the help of acknowledgments, it provides a greater reliability.

3.The flow of bytes transfer can also be informed with the help of acknowledgements that are sent by the receiver to the sender.

4. It allows multiplexing which means that many processes within a single host can use the facilities of TCP communication.

5. It provides a full duplex mechanism which means that the data can be transferred in both directions at the same time.

Some of the key differences are listed below in the table:

	TCP	**UDP**
Stands for:	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Type of Connection:	It is a connection oriented protocol	It is a connection less protocol
Usage:	TCP is used in case of applications in which fast transmission of data is not required	UDP is preferred in case of the applications which have the priority of sending the data on time and on faster rates
Examples:	HTTP, FTP, SMTP Telnet etc	DNS, DHCP, TFTP, SNMP, RIP, VOIP etc
Ordering of data packets:	It rearranges data packets in the order specified	No inherent ordering, the data packets of same message may be ordered differently
Speed of transfer:	Comparatively slow	Comparatively fast
Reliability:	Reliable (defines that data will be definitely sent across)	Unreliable

Header Size:	TCP header size is 20 bytes	UDP Header size is 8 bytes
Fields:	1. Sequence Number, 2. AcK number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer, 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port.	1. Length, 2. Source port, 3. Destination port, 4. Check Sum.
Streaming of data:	Data is read as a byte stream, thus no distinguishing indications are transmitted to the signal message	Packets are sent individually and after the arrival the packets are rearranged
Weight:	It is heavier as it 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 due to no ordering of messages, no tracking connections, etc.
Data Flow Control:	TCP controls the flow of data	UDP does not have an option for flow control

Some of the key differences have been listed in the table below:-

	TCP	**IP**
Definition	TCP provides the service of exchanging data between applications	IP handles addressing and routing messages to the computers across one or more networks
Connection	Connection Oriented	Connection less method

location	Transport	Internet
Reliability	Reliable	Unreliable
Transfer	Segments to internet layer	Datagrams to physical level
Flow control	Yes	No
Format	TCP segments have a 20 byte header with >= 0 bytes of data	IP datagrams contain a message, or one fragment of a message, that may be up to 65,535 bytes (octets) in length

Types of Attacks

Attacks can be categories in two: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Active attack:

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing: When a malicious node miss-present his identity, so that the sender change the topology

b. Modification: When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole: This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network [1].

d. Fabrication: A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices [2].

e. Denial of services: In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole: Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.

g. Sybil: This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

a. Traffic analysis: In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping: This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

c. Monitoring: In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

Advance attacks

a. **Black hole attack:** Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

b. Rushing attack: In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

c. Replay attack: It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

d. Byzantine attack: A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

e. Location disclosure attack: Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

Classes of Malicious Software

Two of the most common types of malware are viruses and worms. These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies. To be classified as a virus or worm, malware must have the ability to propagate. The difference is that a worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself. These and other classes of malicious software are described below.

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer

through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. More advanced worms leverage encryption, wipers, and ransomware technologies to harm their targets.

Trojans

A Trojan is another type of malware named after the wooden horse that the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create backdoors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet.

Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information, such as web crawlers, or interact automatically with Instant Messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s).

In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch Denial of Service (DOS) Attacks, relay spam, and open backdoors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector and are often modified within hours of publication of a new exploit. They have been known to exploit backdoors opened by worms and viruses, which allows them to access networks that have good perimeter control. Bots rarely announce their presence with high scan rates that damage network infrastructure; instead, they infect networks in a way that escapes immediate notice.

Advanced botnets may take advantage of common internet of things (IOT) devices such as home electronics or appliances to increase automated attacks. Crypto mining is a common use of these bots for nefarious purposes.