1. What is wireshark?

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) both are protocols of the Transport Layer. TCP is a connection-oriented protocol where as 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.

**Transmission Control Protocol (TCP)**

[TCP (Transmission Control Protocol)](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/) 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.

**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 takes into account the level of congestion in the network.

**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 OS.
* 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.
* Not suitable for LAN and PAN Networks.
* 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)](https://www.geeksforgeeks.org/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)](https://www.geeksforgeeks.org/routing-information-protocol-rip/).
* Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

**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.

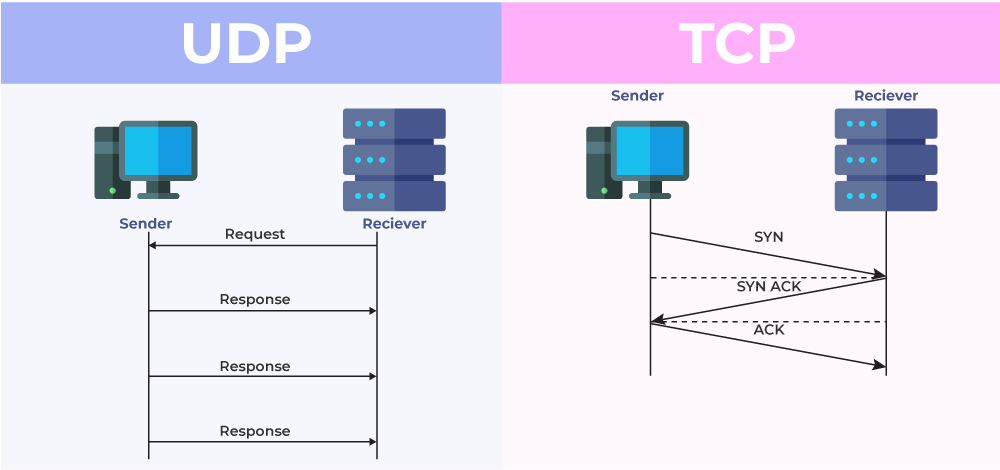
**Disadvantages of UDP**

* We can not 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.

**Which Protocol is Better: TCP or UDP?**

The answer to this question is difficult because it totally depends on what work we are doing and what type of data is being delivered. UDP is better in the case of online gaming as it allows us to work lag-free. TCP is better if we are transferring data like photos, videos, etc. because it ensures that data must be correct has to be sent.

In general, both TCP and UDP are useful in the context of the work assigned by us. Both have advantages upon the works we are performing, that’s why it is difficult to say, which one is better.



*Difference Between TCP and UDP*

**Where TCP is Used?**

* Sending Emails
* Transferring Files
* Web Browsing

**Where UDP is Used?**

* Gaming
* Video Streaming
* Online Video Chats

**Differences between TCP and UDP**

The main differences between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are:

| **Basis** | **Transmission Control Protocol (TCP)** | **User Datagram Protocol (UDP)** |
| --- | --- | --- |
| Type of Service | [TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-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](https://www.geeksforgeeks.org/user-datagram-protocol-udp/)is the Datagram-oriented protocol. This is because  there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission. |
| Reliability | 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. |
| Error checking mechanism | TCP provides extensive error-checking mechanisms.  It is because it provides flow control and acknowledgment of data. | UDP has only the basic error-checking mechanism using checksums. |
| Acknowledgment | An acknowledgment segment is present. | No acknowledgment segment. |
| Sequence | 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. |
| Speed | TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| Retransmission | 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). |
| Header Length | TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| Weight | TCP is heavy-weight. | UDP is lightweight. |
| Handshaking Techniques | Uses handshakes such as SYN, ACK, SYN-ACK | It’s a connectionless protocol i.e. No handshake |
| Broadcasting | TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |
| Protocols | TCP is used by [HTTP, HTTPs](https://www.geeksforgeeks.org/difference-between-http-and-https-2/),[FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/), [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) and [Telnet](https://www.geeksforgeeks.org/introduction-to-telnet/). | UDP is used by [DNS](https://www.geeksforgeeks.org/details-on-dns/), [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/), TFTP, [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/), [RIP](https://www.geeksforgeeks.org/routing-information-protocol-rip/), and [VoIP](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/). |
| Stream Type | The TCP connection is a byte stream. | UDP connection is a message stream. |
| Overhead | Low but higher than UDP. | Very low. |
| Applications | This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services. | This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc. |

**Example:**Suppose there are two houses, H1 and H2, and a letter has to be sent from H1 to H2. But there is a river in between those two houses. Now how can we send the letter?   
**Solution 1:** Make a bridge over the river and then it can be delivered.   
**Solution 2:** Get it delivered by a pigeon.

* Consider the first solution as **TCP**. A connection has to be made (bridge) to get the data (letter) delivered. The data is reliable because it will directly reach another end without loss of data or error.
* The second solution is **UDP**. No connection is required for sending the data. The process is fast as compared to TCP, where we need to set up a connection(bridge). But the data is not reliable: we don’t know whether the pigeon will go in the right direction, will drop the letter on the way, or some issue is encountered mid-travel.

**What is netanim ?**

**Network simulator** is a tool used for simulating the real world network on one computer by writing scripts in C++ or Python. Normally if we want to perform experiments, to see how our network works using various parameters. We don’t have required number of computers and routers for making different topologies. Even if we have these resources it is very expensive to build such a network for experiment purposes.

Using NS3 we can create PointToPoint, Wireless, CSMA, etc connections between nodes. PointToPoint connection is same as a LAN connected between two computers. Wireless connection is same as WiFi connection between various computers and routers. CSMA connection is same as bus topology between computers. After building connections we try to install NIC to every node to enable network connectivity.

What is ftp?

The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.

What is ns3 ?

ns is a name for a series of discrete event network simulators, specifically ns-1, ns-2, and ns-3. All are discrete-event computer network simulators, primarily used in research and teaching

TOPOLOGY :

There are mainly eight types of topology in computer networks:

1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology
6. P2P Topology

**Mesh Topology**

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

There are two types of Mesh topology:

1. **Full Mesh Topology:** In this topology each device is connected to all the devices available on the network.
2. **Partial Mesh Topology:** In partial mesh topology, each device is connected to only those devices, to which they communicate frequently. This reduces redundant links and saves the setup cost.

**Advantages of Mesh topology**

1. **No data loss:** No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.  
2. **Reliable:** Mesh topology is reliable and robust as failure of one link doesn’t affect other links and the communication between other devices on the network.  
3. **Secure:** Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.  
4. **Easy to troubleshoot:** Fault detection is easy as there is a separate connection between each devices.  
5. **Fast communication:** As there is a dedication connection between two devices on a network, the communication is fast.

**Disadvantages of Mesh topology**

1. Amount of wires required to connected each system is tedious and headache.  
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.  
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

**Star Topology**

In star topology each device in the network is connected to a central device called **hub**. Unlike Mesh topology, star topology doesn’t allow direct communication between devices, a device must have to communicate through hub.

If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

The **central device is known as hub** and **other devices connected to hub are called clients**. Generally Coaxial cable or RJ-45 cables  are used to connect the clients to the hub.

**Advantages of Star topology**

* **Less expensive:** Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
* **Easier to install**
* **Cost effective:** Less amount of cables required because each device needs to be connected with the hub only.
* **Robust:** If one link fails, other links will work just fine.
* **Easy to troubleshoot:** Easy fault detection because the link can be easily identified.
* **Reliable:** Each device is separately connected to the hub, so a connection failure between a device and hub doesn’t affect the connection of the other devices.

**Disadvantages of Star topology**

* If hub goes down everything goes down, none of the devices can work without hub.
* Hub requires more resources and regular maintenance because it is the central system of star topology.
* **Not Scalable:**There is a limit to add new devices as each device increase the load on the central unit (hub or switch). This is why it is not suitable for the large networks.

**Bus Topology**

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

* The main cable that is connected to the devices on the network using drop line is called **backbone cable**.
* The main cable **broadcast the message** to all the devices connected to it.
* When a device wants to sends a message, it **transmits the message to the backbone cable**. All the other devices connected to the backbone cable receives the message whether they are intended to receive the message or not.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access). This method is used to prevent the collision of data as two or more devices can send the data to main cable at the same time.

**CSMA:** This method is developed to decrease the chance of collisions when two or more devices starts sending the signal at the same time.

**CSMA CD (Carrier Sense Multiple Access with Collision Detection):**In this method, a device monitors the transmission medium after it sends the data to see if the transmission was successful. If successful, the device marks the communication successful else it sends the data again.  
**CSMA CA (Carrier Sense Multiple Access with Collision Avoidance):** This method tries to prevent the collision from happening. In this method, before sending the data, the device checks the transmission medium to see if it is busy or not. If busy, then the sender device waits until the transmission medium becomes idle.

**Advantages of bus topology**

* **Easy installation**, each cable needs to be connected with backbone cable.
* **Less Expensive:** **Less cables** are required than Mesh and star topology
* **Limited failure:** The connection failure of one device doesn’t affect the connections of other devices on network.

**Disadvantages of bus topology**

* Difficultly in fault detection.
* **Not scalable** as there is a limit of how many nodes you can connect with backbone cable.
* **Difficult to troubleshoot:** It is difficult to identify the cause of failure.
* **Data collision:** When two or more devices send the data simultaneously then there is a chance of data collision. However this can be solved by implementing CSMA techniques that we discussed above.

**Ring Topology**

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as **ring topology**.

If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

* Data flow is **unidirectional** in ring topology.
* This topology doesn’t have any end points as nodes are connected in circular fashion.
* The data transfers in ring topology in clockwise direction.
* The popular access method used in ring topology is **token passing method.**The word token describes segment of data send through the network. There are multiple tokens available on the network, the device that successfully acquires the token attaches the data to the token. The device that successfully decodes the token, receives the data.

**Advantages of Ring Topology**

* Easy to install.
* Managing is easier as to add or remove a device from the topology only two links are required to be changed.
* **Less expensive:** Generally Twisted pair cabling is used in ring topology which is inexpensive and easily available.
* **Easy maintenance:** The network in ring topology is easy to maintain as a system failure doesn’t affect other systems on network, the failed system can be easily removed and installed again after fixing the issue.

**Disadvantages of Ring Topology**

* A link failure can fail the entire network as the signal will not travel forward due to failure.
* Data traffic issues, since all the data is circulating in a ring.

**Hybrid topology**

A combination of two or more topology is known as hybrid topology. For example a combination of star and bus topology is known as star bus hybrid topology, this topology is shown in the above diagram.

**Advantages of Hybrid topology**

* We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
* Scalable as we can further connect other computer networks with the existing networks with different topologies.

**Disadvantages of Hybrid topology**

* Fault detection is difficult.
* Installation is difficult.
* Design is complex so maintenance is high thus expensive.

**P2P (Peer to Peer) Topology**

In Peer to Peer topology, two devices are connected to each other directly. There is no client and server in P2P topology as both the devices serve the purpose of client and server both. **Torrent is an example of P2P topology** as one computer can download the data as well as upload the data to another computer.

In P2P, these two devices can be two computers, routers, switches etc. The client is the computer that requests the data and server is the computer that serves the request by sending data. In P2P, both the devices can request as well as send the data.

**Con:** The biggest disadvantage of P2P network is the security. A computer connected to another computer using P2P can read and write the data on the computer.

Difference between Star and Mesh Topology:

| **Star Topology** | **Mesh Topology** |
| --- | --- |
| In [star topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/), the nodes are connected to the central hub or router. | In[mesh topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology/), the nodes are connected to each other completely via dedicated link. |
| There are N links in Star topology, if there are N nodes. | There are N(N-1)/2 links in Mesh topology, if there are N nodes. |
| The cost of Star topology is less. | The cost of Mesh topology is expensive. |
| The complexity of Star topology is quite simple. | The complexity of Mesh topology is complex. |
| In star topology, the information is travel from central hub or router to all the nodes. | In mesh topology, the information is travel from nodes to nodes. |
| Star topology is very good extensible. | Mesh topology is poor extensible. |
| In star topology, twisted pair cable is used for connection. | In mesh topology, twisted pair cable, coaxial cable and optical fiber cable are used for connection on the basis of type of networks. |
| Star topology is used in LAN as setup is easy. | Mesh topology is used in WAN. |
| It is less robust as compared to mesh topology. | It is highly robust. |
| The breakdown of central hub leads to failure of entire network. | The breakdown of a node does not affect other nodes in  a network. |
| It is easy to install and reconfigure. | It is difficult to install and reconfigure because of extensive cabling. |

**How to start stop and restart the service ?**

**Starting a Linux service**

Let’s say you want to start the Apache server.

To do this:

1. Open a terminal window.

2. Run the command sudo systemctl start httpd.

In this command:

* sudo tells Linux you are running the command as the root user.
* systemctl manages systemd services.
* start tells the systemctl command to start the Apache service.
* httpd is the name of the Apache web server service.

3. Once you run the command you will get the following message:

The service httpd has started successfully.

**Note** that if the service is already running you will see the following message:

The service httpd is already running.

**Stopping a Linux service**

To stop the Apache service:

1. Open a terminal window

2. Run the command sudo systemctl stop httpd.

3. You should now see the following message:

The service httpd has been stopped successfully.

Note that if the service, in this case Apache, was not running you will get the following message:

Failed to stop service httpd. Unit httpd.service is not loaded.

Or you may get one of the following messages:

Failed to stop service httpd. Unit httpd.service is not running.

Failed to stop service httpd. Unit httpd.service is in a failed state.

Failed to stop service httpd. Unit httpd.service is locked.

**Restarting a Linux service**

To restart the same service (Apache):

1. Open a terminal window.

2. Run the command sudo systemctl restart httpd.

3. The service will restart, and you’ll be returned to the bash prompt.

4. You will get the following message:

The service httpd has been restarted successfully.

If the service isn’t running, you’ll see the following output:

The service httpd is not running.

You can also use the following command to check the status of the service before you try to restart it:

systemctl status httpd

What is simulation?

A simulation is the imitation of the operation of a real-world process or system over time. Simulations require the use of models; the model represents the key characteristics or behaviors of the selected system or process, whereas the simulation represents the evolution of the model over time.

## Definition of hubs

A hub is a network device that connects various network nodes, e.g. in an Ethernet, in a star configuration. In the OSI (Open Systems Interconnections) reference model, hubs are classified as level 1 devices that operate at the physical layer. Their main task is to interconnect several computers and immediately forward received data. Hubs are usually made of plastic, run on an external power supply and contain between 4 and 16 ports, i.e. physical connections. Their maximum bandwidth is usually 10/100 Mbit per second.

## How does a hub work?

A hub receives data and then sends it in full to all connected devices (hosts). All ports of the hub operate at the same speed and are located in a collision domain (which includes all connected network devices). Unlike other network devices, a hub does not offer the option to control or exclude only individual receivers. This means that **all data packets are always forwarded to all computers** during a transfer. This means that even those devices the data wasn’t intended for also receive the data. Since all hosts are occupied in this way, the other devices cannot send any data themselves in the meantime. Instead, simultaneous requests are processed one after the other.

If you need more hosts, you can connect one hub to another hub. This connection is created with a simple crossover cable over one of the ports. However, the number of hosts is **automatically limited by the 5-4-3 rule,** or repeater rule. This states that a maximum of five segments with four repeaters can be used between two end devices. In addition, the connected hosts share the entire bandwidth when a hub is used. This inevitably leads to speed losses, especially when transferring large data packets.

What is 3 way handshake ?

A three-way handshake (TCP/IP handshake) is the first three interactions between a client and a server trying to establish a TCP connection. These initial interactions are essential in making a secure connection. At this phase, both client and server will agree on parameters that they will use to check and verify incoming and outgoing packets of data. These parameters will be in the form of TCP segments.