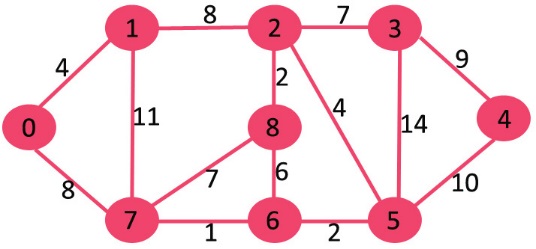
Dijkstra’s shortest path algorithm

Below are the detailed steps used in Dijkstra’s algorithm to find the shortest path from a single source vertex to all other vertices in the given graph.  
Algorithm  
**1)** Create a set *sptSet* (shortest path tree set) that keeps track of vertices included in shortest path tree, i.e., whose minimum distance from source is calculated and finalized. Initially, this set is empty.  
**2)** Assign a distance value to all vertices in the input graph. Initialize all distance values as INFINITE. Assign distance value as 0 for the source vertex so that it is picked first.  
**3)** While *sptSet* doesn’t include all vertices  
….**a)** Pick a vertex u which is not there in *sptSet* and has minimum distance value.  
….**b)** Include u to *sptSet*.  
….**c)** Update distance value of all adjacent vertices of u. To update the distance values, iterate through all adjacent vertices. For every adjacent vertex v, if sum of distance value of u (from source) and weight of edge u-v, is less than the distance value of v, then update the distance value of v.

Let us understand with the following example:  
[](https://www.geeksforgeeks.org/wp-content/uploads/Fig-11.jpg)

The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with minimum distance value. The vertex 0 is picked, include it in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8. Following subgraph shows vertices and their distance values, only the vertices with finite distance values are shown. The vertices included in SPT are shown in green colour.

[](https://www.geeksforgeeks.org/wp-content/uploads/MST1.jpg)

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.

[](https://www.geeksforgeeks.org/wp-content/uploads/DIJ2.jpg)

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).  
[](https://www.geeksforgeeks.org/wp-content/uploads/DIJ3.jpg)

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.

[](https://www.geeksforgeeks.org/wp-content/uploads/DIJ4.jpg)

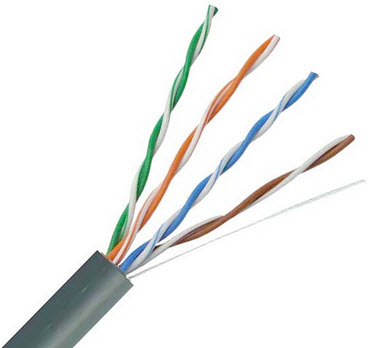
We repeat the above steps until sptSet doesn’t include all vertices of given graph. Finally, we get the following Shortest Path Tree (SPT).

[](https://www.geeksforgeeks.org/wp-content/uploads/DIJ5.jpg)

### Types of Ethernet Networks

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switch Ethernet. A network is a group of two or more computer systems connected together.

**1. Fast Ethernet**

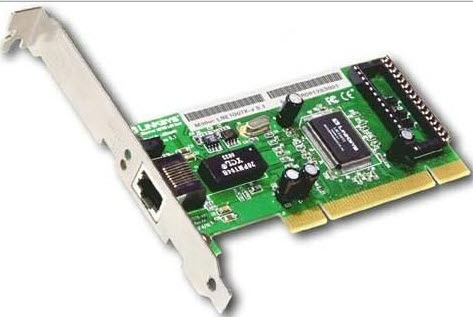
[](https://www.elprocus.com/wp-content/uploads/2014/02/39.jpg)Twisted pair cable

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable. The older 10 Mbps Ethernet is still used, but such networks do not provide necessary bandwidth for some network-based video applications.

Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol, and uses existing 10BaseT cabling. Data can move from 10 Mbps to 100 Mbps without any protocol translation or changes to the application and networking software.

**What is Ethernet Port Speed?**

When compare to a 10 mb port, a 100 Mb port is theoretically 10 times faster than the standard port. Therefore, with a 100 Mb port more information can stream to and from your server. This will be of great help to you if you really need to explore very high speed, but not if you are under DDOS attack because you will find yourself running out of traffic allocation very fast.

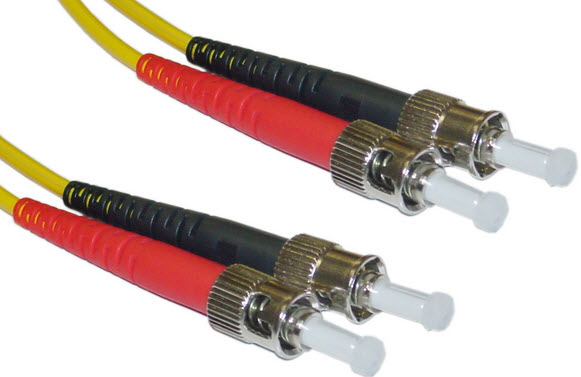
[](https://www.elprocus.com/wp-content/uploads/2014/02/82.jpg)100Mbit/s Ethernet port

If you are doing standard web hosting, the bigger 100 Mbps pipe will not offer true benefit to you because you may not even use more than 1 mbps at any given time. If you are hosting games or streaming media, then the bigger pipe of 100 Mbps would indeed be helpful to you.

With a 10 mbps pipe, you can transfer up to 1.25 Mbps, while a 100 mbps pipe, would allow you to transfer up to 12.5 Mbps.

However, if you leave your server unattended and running at full steam, a 10 Mbps pipe can consume about 3,240 GB a month and a 100 Mbps pipe can consume up to 32,400 GB a month. It would be really disgusting when you receive your bill.

**2. Gigabit Ethernet**

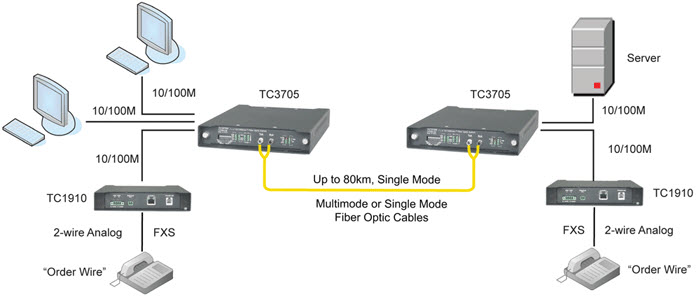
[](https://www.elprocus.com/wp-content/uploads/2014/02/411.jpg)Optic fiber cable

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular. The type of twisted-pair cables that support Gigabit Ethernet is Cat 5e cable, where all the four pairs of twisted wires of the cable are used to achieve high data transfer rates. The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

**3. Switch Ethernet**

Multiple network devices in a LAN require network equipments such as a network switch or hub. When using a network switch, a regular network cable is used instead of a crossover cable. The crossover cable consists of a transmission pair at one end and a receiving pair at the other end.

The main function of a network switch is to forward data from one device to another device on the same network. Thus a network switch performs this task efficiently as the data is transferred from one device to another without affecting other devices on the same network.

[](https://www.elprocus.com/wp-content/uploads/2014/02/58.jpg)Switch Ethernet

The network switch normally supports different data transfer rates. The most common data transfer rates include 10 Mbps – 100 Mbps for fast Ethernet, and 1000 Mbps – 10 Gbps for the latest Ethernet.

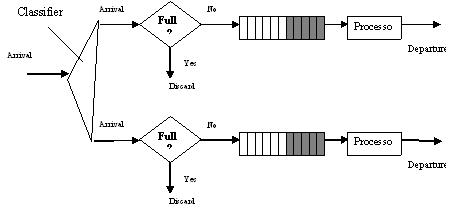
Switch Ethernet uses star topology, which is organized around a switch. The switch in a network uses a filtering and switching mechanism similar to the one used by the gateways, in which these techniques have been in use for a long time.

**QoS (Quality of Service)**

refers to a broad collection of networking technologies and techniques.  The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results.  Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.  
            QoS involves prioritization of network traffic.  QoS can be targeted at a network interface, toward a given server or router’s performance, or in terms of specific applications.  A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.  
            QoS is especially important for the new generation of Internet applications such as VoIP video-on-demand and other consumer services.  
            Some core networking technologies like Ethernet were not designed to support prioritized traffic or guaranteed of performance levels, making it much more difficult to implement QoS solutions across the Internet.  
            Quality of Service is an internetworking issue that has to be defined as something a flow seeks to attain.

**Technique to improve QoS:**  
            There are many techniques used to improve the quality of service. Some common methods are,  
**Scheduling:**   Packets from different flows arrive at a switch or router for processing.  A good scheduling technique treats the different flows in a fair and appropriate manner.  Some of the scheduling techniques used to improve QoS are,

* FIFO Queuing:  In this queuing technique, the arrival packets are stored in **First Come First Serve**basis.  If the arrival rate is less than the processing rate, then the queue will fill up and the new arriving packets will not have any space to store in the queue and gets discarded.
* Priority Queuing - In priority queuing packets are first assigned to a priority class.  Each priority class has its own queue.  The packets in the highest priority queue are processed first.  The packets in the lowest priority queue are processed last.  This process continues until the queue is empty.



Advantage:  It provides better QoS for higher priority traffic such as multimedia that can reach the destination with less delay.  
Disadvantage: At any situation, the higher priority queue has continuous packet flow then the lower priority queue never get a chance to process.  It is called as “**Starvation**”.

* Weighted Fair Queuing – In Weighted Fair Queuing technique, the packets are still assigned to different classes and admitted to different queues.  However, the queues are weighted based on the priority of the queues (higher priority means a higher weight).  The system processes packets in each queue in a round robin fashion with the number of packets selected from each queue based on the corresponding weight.

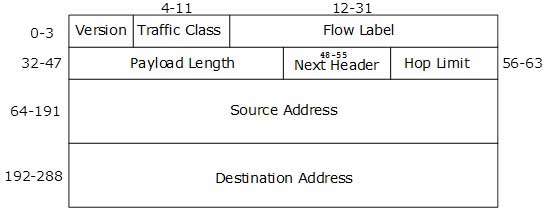
**Traffic Shaping:**

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.  There are two techniques under this mechanism.

* Leaky Bucket – If the traffic consists of fixed size packets, the process removes a fixed number of packets from the queues.  If the traffic consists of variable length packets, the fixed output rate must be based on the number of bytes or bits.
* Token Bucket – Leaky bucket algorithm outputs the data in average rate from the burst data, but it does not taken the time when the host was idle, into account.

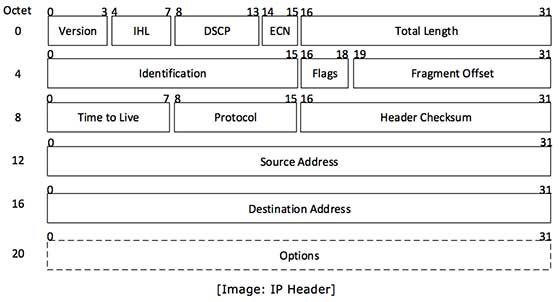
But, the Token Bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens.  For each tick of the clock, the system sends ‘n’ token to the bucket.  The system removes one token for every cell (or byte) of data sent.  
**Admission Control:**  
            It is a mechanism used by the networking device like router and switches to accept or reject a flow based on predefined parameters called flow specification.  Before a router accepts a flow for processing, it checks the flow specification to see if its capacity and its previous commitments to other flows can handle the new flow.  
**Resource reservation:**  
      A flow of data needs resource such as buffer bandwidth, CPU time and so on.  The QoS is improved if these resources are reserved beforehand.

IPv6 header



|  |  |
| --- | --- |
| 1 | **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110. |
| 2 | **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN). |
| 3 | **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media. |
| 4 | **Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0. |
| 5 | **Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4’s. |
| 6 | **Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded. |
| 7 | **Source Address** (128-bits): This field indicates the address of originator of the packet. |
| 8 | **Destination Address** (128-bits): This field provides the address of intended recipient of the packet. |

**IPV4 Header**



IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

* **Version:** Version no. of Internet Protocol used (e.g. IPv4).
* **IHL:** Internet Header Length; Length of entire IP header.
* **DSCP:** Differentiated Services Code Point; this is Type of Service.
* **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
* **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
* **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
* **Flags:** As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.
* **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
* **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
* **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
* **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
* **Source Address:** 32-bit address of the Sender (or source) of the packet.
* **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
* **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

**Classful addressing:**In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.Each of the IP address belongs to a particular class that's why they are classful addresses.Earlier this addressing system did not have any name,but when classless addressing system came into existence then it is named as Classful addressing system.The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device.One of the major disadvantage of classful addressing is that it does not send subnet information but it will send the complete network address. The router will supply its own subnet mask based on its locally configured subnets. As long as you have the same subnet mask and the network is contiguous, you can use subnets of a classful network address.

**Classless Addressing:**Classless addressing system is also known as CIDR(Classless Inter-Domain Routing).Classless addressing is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes.What happened in classful addressing is that if any company needs more than 254 host machines but far fewer than the 65,533 host addresses then the only option for the company is to take the class B address.Now suppose company needs only 1000 IP addresses for its host computers then in this (65533-1000=64533) IP addresses get wasted.For this reason, the Internet was, until the arrival of CIDR, running out of address space much more quickly than necessary. CIDR effectively solved the problem by providing a new and more flexible way to specify network addresses in routers.A CIDR network address looks like this: