**Unit-III**

Introduction

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

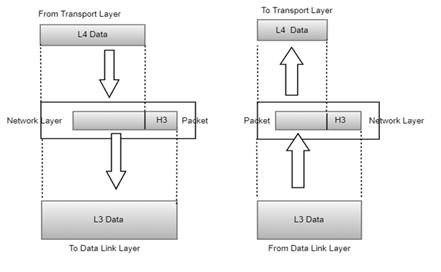
Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

**Functions of Network Layer**

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

Before learning about design issues in the network layer, let’s learn about its various functions.

* **Addressing** – Maintains both the source and destination addresses at the frame header. The network layer performs addressing to find out the specific devices on the network.
* **Packetizing** – The network layer works on the conversion of packets those received from its upper layer. This feature is accomplished by Internet Protocol (IP).
* **Routing** – Being considered as the major functionality, the network layer chooses the best path for data transmission from a source point to the destination.
* **Internetworking** – Internetworking works to deliver a logical connection across multiple devices.



* Addressing devices and networks.
* Populating routing tables or static routes.
* Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
* Internetworking between two different subnets.
* Delivering packets to destination with best efforts.
* Provides connection oriented and connection less mechanism.

**Network Layer Features**

With its standard functionalities, Layer 3 can provide various features as:

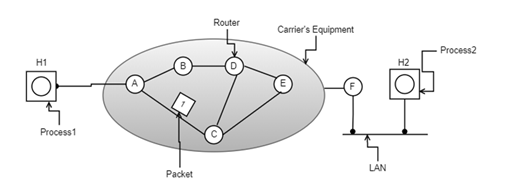
* Quality of service management
* Load balancing and link management
* Security
* Interrelation of different protocols and subnets with different schema.
* Different logical network design over the physical network design.
* L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Network Layer Design Issues

Network layer comes up with certain design issues and they can be described as below:

1. **Store-and-Forward Packet Switching**

Here, the foremost elements are the carrier’s equipment (the connection between routers through transmission lines) and the customer’s equipment.



store-and-forward packet switching

* H1 has a direct connection with carrier router ‘A’, while H2 is connected to carrier router ‘F’ on a LAN connection.
* One of the carrier router ‘F’, is pointed outside the carrier’s equipment as it does not come under the carrier, whereas considered as protocols, software, and construction.
* This switching network performs as Transmission of data happens when the host (H1) with a packet transfers it to the nearby router through [LAN](https://www.elprocus.com/application-specific-integrated-circuits/) (or) point-to-point connection to the carrier. The carrier stores the packet until it completely arrives thus confirms the checksum.
* Then after, the packet is transmitted over the path until H2 is reached.

1. **Services Provided to the Transport Layer**

Through the network/transport layer interface, the network layer delivers its services to the transport layer. One might come across the question of what type of services does the network layer provides?

So, we shall move with the same query and find out the services offered.

Services offered by the network layer are outlined considering few objectives. Those are:

* Offering services must not depend on router technology
* The transport layer needs to be protected from type, number and the topology of the available routers.
* Network addressing the transport layer needs to follow a consistent numbering scenario also at LAN and WAN connections.

**Note**: Next comes the scenario of connection-Oriented or connectionless

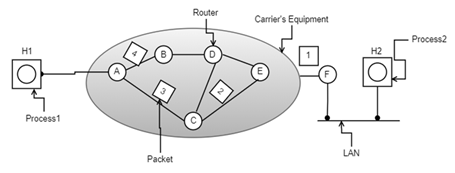
Here, two groupings are possible based on the offered services.

**Connectionless** – Here, routing and insertion of packets into subnet is accomplished individually. No additional setup is necessary

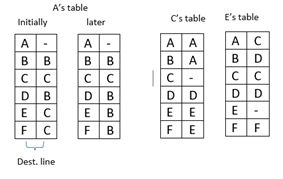
**Connection**-**Oriented** – Subnet must offer reliable service and all the packets are transmitted over a single route.

1. **Implementation of Connectionless Service**

In this scenario, packets are termed as datagrams and the corresponding subnet is termed as datagram subnet. Routing in datagram subnet is as follows:



datagram subnet



truth table

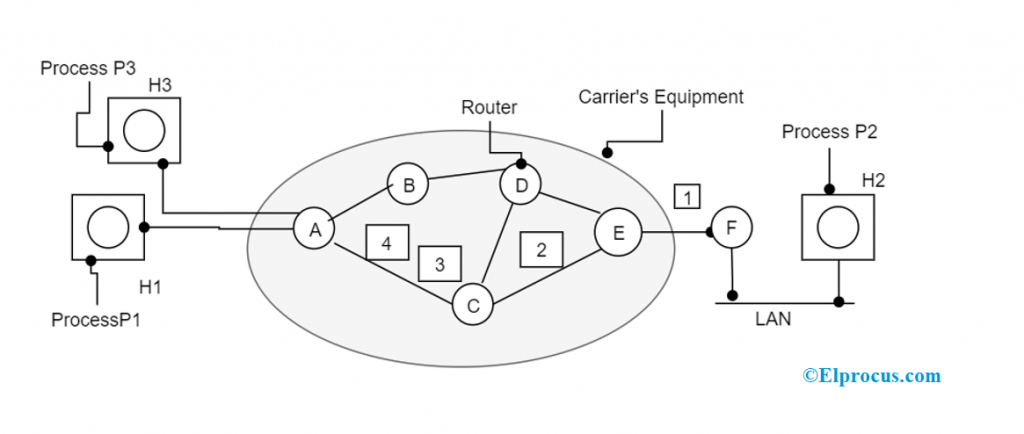
When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and then transmits each packet to router ‘A’ through a few protocols. Each router is provided with a routing table where it decides the destination points.  
In the above figure, it is clear that packets from ‘A’ need to be transmitted either to B or C even when the destination is ‘F’. The routing table of ‘A’ is clearly outlined above.

Whereas in the case of packet 4, the packet from ‘A’ is routed to ‘B’, even the destination node is ‘F’. Packet ‘A’ chooses to transmit packet 4 through a different path than the initial three paths. This might happen because of traffic congestion along the path ACE. So, the

1. **Implementation of Connection-Oriented Service**

Here, the functionality of connection-oriented service works on the virtual subnet. A virtual subnet performs the operation of avoiding a new path for each packet transmission. As a substitute for this, when there forms a connection, a route from a source node to a destination node is selected and maintained in tables. This route performs its action at the time of traffic congestion.

At the time when the connection is released, the virtual subnet also gets dismissed. In this service, every packet carries its own identifier that states the exact address of the virtual circuit. The below diagram shows the [routing algorithm](https://www.elprocus.com/application-specific-integrated-circuits/) in the virtual subnet.

Implementation of Connection-Oriented Service

Network Layer Routing Protocols

Network routing protocols are of many types. All the protocols are described below:

1. **Routing Information Protocol -** This protocol is mainly implemented in the LAN and WAN network. Here, it is classified as an interior gateway protocol internal to the utilization of a distance-vector algorithm.
2. **Interior Gateway Routing Protocol -** This protocol is used for routing of information internal to the independent system. The main aim behind this protocol is to annihilate the limitations of RIP in the complicated networks. It even manages various metrics for every path along with consistency, bandwidth and delay load. The greatest hop is of 255 and routing updates are transmitted at the rate of 90 seconds.
3. **Open Shortest Path First -** It is considered as the active routing protocol mostly utilized in internet protocols. Especially, it is the link-state routing protocol and moves into the classification of interior gateway protocol.
4. **Exterior Gateway Protocol -** The best routing protocol chosen for internet activity is the exterior gateway protocol. It has a different scenario when compared with path and distance vector protocols. This protocol follows the topology like that of a tree.
5. **Enhanced Interior Gateway Routing Protocol -** It is the distance-vector routing protocol in improvement in the optimization decreasing instability in routing that happens after topology modification, in addition to the usage of bandwidth and processing capability. In general, optimization is dependent on DUAL work from SRI that makes sure of the loop-free process and provides scope for a quick junction.
6. **Border Gateway Protocol -** This protocol is responsible for the maintenance of a table of internet protocol networks that manage network approaching ability between AS. This is articulated in the form of a path vector protocol. Here, general IGP metrics are not implemented but goes with decisions depending on the path and network rules.
7. **Intermediate System-to-Intermediate System -** This is mostly employed by network devices where it decides the best method for the transmission of a datagram and this scenario id termed as routing.

**Network Layer Services**

The network layer provides services that permit end devices for information exchange across the network. To achieve this, it makes use of four processes where those are of

Addressing end devices

* Encapsulation
* Routing
* De-encapsulation

With all the routing protocols, types, services, and other frameworks, the network layer stands as a great support for the OSI model. The functionality of the network layer contains in every router. The most general protocols that are in relation to the network layer are [Internet protocol](https://en.wikipedia.org/wiki/Internet_Protocol) and Netware IPX/SPX. As network layer been in implementation by many organizations, learn deeper insights on what are the approaches that network layer is associated with?

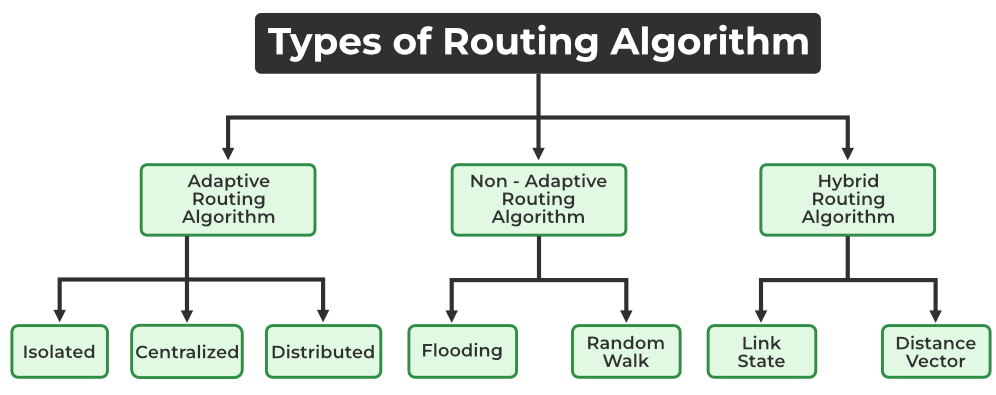
Routing Algorithms

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

**Classification of Routing Algorithms**

The routing algorithms can be classified as follows:

1. Adaptive Algorithms
2. Non-Adaptive Algorithms
3. Hybrid Algorithms



*Types of Routing Algorithm*

1. **Adaptive Algorithms**

These are the algorithms that change their [routing](https://www.geeksforgeeks.org/types-of-routing/) decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.

Further, these are classified as follows:

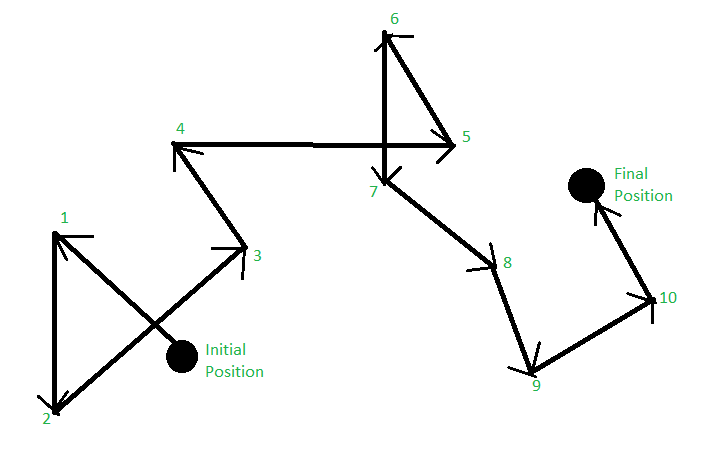
* **Isolated:** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes don’t have information about the status of a particular link. The disadvantage is that packets may be sent through a congested network which may result in delay. Examples: Hot potato routing, and backward learning.
* **Centralized:** In this method, a centralized node has entire information about the network and makes all the routing decisions. The advantage of this is only one node is required to keep the information of the entire network and the disadvantage is that if the central node goes down the entire network is done. The link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
* **Distributed:** In this method, the node receives information from its neighbors and then takes the decision about routing the packets. A disadvantage is that the packet may be delayed if there is a change in between intervals in which it receives information and sends packets. It is also known as a decentralized algorithm as it computes the least-cost path between source and destination.
* **Advantages of Adaptive Routing Algorithms:**
* **Dynamic**: Adaptive routing algorithms can adjust to changing network conditions, such as traffic congestion, link failures, and topology changes, by selecting a better path for the data packets. This results in better network performance, higher throughput, and reduced latency.
* **Load Balancing**: Adaptive routing algorithms can distribute network traffic across multiple paths to avoid congestion and ensure that all network links are utilized efficiently.
* **Fault Tolerance**: Adaptive routing algorithms can reroute data packets around network failures, which enhances network availability and reliability.
* **Better Performance**: Adaptive routing algorithms can provide better network performance by selecting the shortest or the least congested path for the data packets.
* **Disadvantages of Adaptive Routing Algorithms:**
* **Complexity**: Adaptive routing algorithms are more complex than non-adaptive algorithms, which makes them harder to implement and maintain.
* **Overhead**: Adaptive routing algorithms require more processing power and memory to execute, which can lead to increased overhead and resource utilization.
* **Routing Loops**: Adaptive routing algorithms may sometimes result in routing loops, which can cause data packets to be stuck in the network indefinitely.
* **Delay**: Adaptive routing algorithms may introduce additional delay in the network due to the time required to calculate the best path for each data packet.

1. **Non-Adaptive Algorithms**

These are the algorithms that do not change their routing decisions once they have been selected. This is also known as [static routing](https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/)as a route to be taken is computed in advance and downloaded to routers when a router is booted.

Further, these are classified as follows:

* **Flooding:** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.
* **Random walk:** In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.



*Random Walk*

* **Advantages of Non-Adaptive Routing Algorithms:**
* Simplicity: Non-adaptive routing algorithms are simple to implement and maintain, which reduces the cost and complexity of the network infrastructure.
* Low Overhead: Non-adaptive routing algorithms require minimal processing power and memory to execute, which reduces the overhead and resource utilization.
* Avoid Routing Loops: Non-adaptive routing algorithms are less likely to result in routing loops, which reduces the chances of data packets being stuck in the network indefinitely.
* Fast: Non-adaptive routing algorithms can provide faster routing decisions since they do not require the calculation of the best path for each data packet.
* **Disadvantages of Non-Adaptive Routing Algorithms:**
* Inefficient: Non-adaptive routing algorithms may select suboptimal paths for the data packets, which can result in congestion, longer latency, and reduced throughput.
* Inflexible: Non-adaptive routing algorithms cannot adjust to changing network conditions, which may result in network failures, reduced performance, and increased latency.
* Unresponsive: Non-adaptive routing algorithms cannot respond to network faults, which may result in data packet loss and reduced network availability.
* Uneven Traffic Distribution: Non-adaptive routing algorithms may lead to uneven traffic distribution, which may result in some links being underutilized while others are congested.

1. **Hybrid Algorithms**

As the name suggests, these algorithms are a combination of both adaptive and non-adaptive algorithms. In this approach, the network is divided into several regions, and each region uses a different algorithm.

Further, these are classified as follows:

* **Link-state:** In this method, each router creates a detailed and complete map of the network which is then shared with all other routers. This allows for more accurate and efficient routing decisions to be made.
* **Distance vector:** In this method, each router maintains a table that contains information about the distance and direction to every other node in the network. This table is then shared with other routers in the network. The disadvantage of this method is that it may lead to routing loops.

**Difference between Adaptive and Non-Adaptive Routing Algorithms**

The main difference between Adaptive and Non-Adaptive Algorithms is:

* Adaptive Algorithms are the algorithms that change their routing decisions whenever network topology or traffic load changes. It is called Dynamic Routing. Adaptive Algorithm is used in a large amount of data, highly complex network, and rerouting of data.
* Non-Adaptive Algorithms are algorithms that do not change their routing decisions once they have been selected. It is also called static Routing. Non-Adaptive Algorithm is used in case of a small amount of data and a less complex network.

For more differences, you can refer to Differences between Adaptive and Non-Adaptive Routing Algorithms.

**Difference between Routing and Flooding**

The difference between Routing and Flooding is listed below:

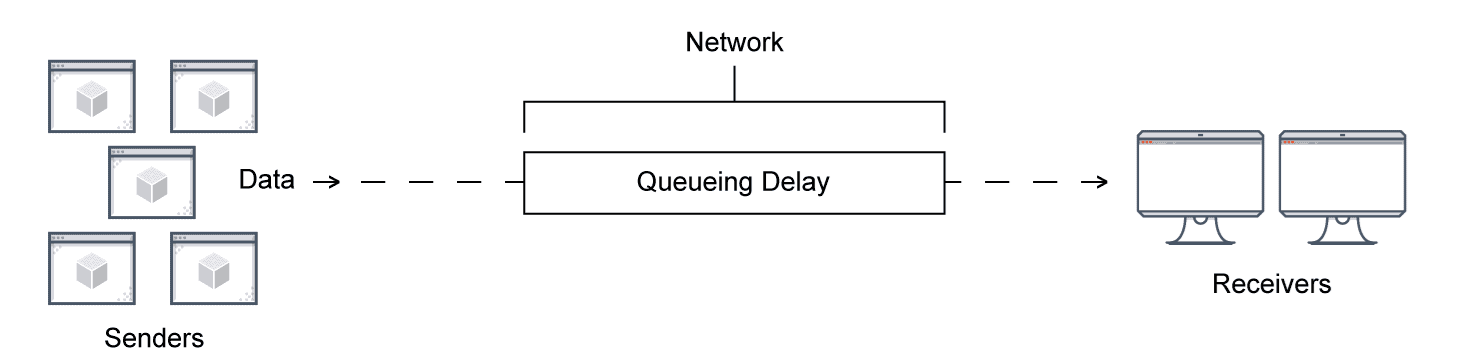
|  |  |  |
| --- | --- | --- |
| **S. No.** | **Adaptive Routing algorithm** | **Non-Adaptive Routing algorithm** |
| 1 | An adaptive algorithm involves routers for exchanging and updating router table data. | A non-adaptive algorithm involves a network administrator for the manual entry of the routing paths into the router. |
| 2 | This algorithm creates a routing table based on network conditions. | Whereas this algorithm creates a static table in order to determine when to send packets and which node. |
| 3 | This algorithm is used by dynamic routing. | Whereas this algorithm is used by static routing. |
| 4 | In adaptive routing algorithm, the routing decisions are made based on network traffic and topology. | Whereas in a non-adaptive routing algorithm, the routing decisions are not made based on network traffic and topology. |
| 5 | Adaptive routing algorithms are more complex as compared to non-adaptive routing algorithms in terms of complexity. | While non-adaptive routing algorithms are simple in terms of complexity. |
| 6 | In adaptive routing algorithm, the routing decisions are not static tables. | While in non-adaptive routing algorithm, the routing decisions are static tables. |
| 7 | Adaptive routing algorithm is categorized into distributed, centralized and isolation algorithm. | Whereas non-adaptive routing algorithm is categorized into random walks and flooding. |
| 8 | Adaptive routing algorithm is more used as compared to non-adaptive. | Whereas non-adaptive routing algorithm is comparatively less used. |
| 9 | The dynamic protocols are employed to update the routing table and determine the best route between the source and destination computers. | The manual setup is performed for establishing an optimal path between the source and destination computers. |
| 10 | It is mostly used for-  Open, Complex network topologies | It is mostly used for-  Simple, Closed network topologies |
| 11 | Purposes-  Enhancement in network performance  Prevents packet delivery failure  Aid in controlling congestion | Purposes-  It enables fine-grained control over packet paths.  Suited for reliable networks with stable loads |

Congestion

Network congestion refers to a reduction in quality of service (QOS) that causes packet loss, queueing delay, or the blocking of new connections. Typically, network congestion occurs in cases of traffic overloading when a link or network node is handling data in excess of its capacity.

To avoid collapse and reduce the effects of congestion in the network, organizations use various congestion avoidance and congestion control methods. These include:

* TCP/IP window reduction
* Fair queueing in network devices such as routers, switches, and other devices
* Priority schemes which transmit higher priority packets ahead of other traffic
* Explicit network resource allocation via admission controls toward specific flows



**Identification of Network Congestion**

There are five ways to identify network congestion:

* **Bandwidth:** The most common cause of network congestion is bandwidth. Bandwidth refers to the ideal capacity of the network to transfer a certain amount of data from a source to a destination in a specific amount of time. A lack of bandwidth can lead to network outages.
* **Latency**: Latency is the time taken to transmit, capture, transmit, and process data from source to destination. It refers to the speed of your network traffic measured in milliseconds. High latency can lead to a slower network. Latency numbers may vary based on the application and network connection usage.
* **Jitter**: Jitter refers to the time delay while sending data packets to a destination from a source over a network. When traffic becomes unpredictable, it causes jitter and network congestion. Jitter can also impact the quality of audio and video quality on your network. Network equipment and devices try to adjust the changes caused by traffic patterns, which creates jitter and leads to congestion as a cascading effect.
* **Packet Retransmission**: Packet retransmission is required when the movement of data packets stops due to packet loss, packet damage, or more. In such cases, data packets are resent from source to destination, increasing network congestion.
* **Collision:** Packet collision occurs when two or more network nodes try to send data simultaneously. This leads to packet loss and requires resending of packets, which can negatively impact network performance. Collision is a back-off process where all the packets have to wait to clear the network congestion. It can be due to an inappropriate connection, poor cabling, and more.

**Causes of Network Congestion**

The first step to troubleshoot network issues such as congestion is to understand and identify their root cause. There can be several causes of network congestion:

* **Unneeded Traffic:** The most common cause of network congestion is unneeded traffic. It may include streaming video content, advertisements, or junk VoIP phone calls that consume bandwidth. It’s important to identify unneeded traffic before it slows down your network.
* **Misconfigured Traffic:** Business traffic typically comes from multiple sources.
  + Unicast traffic to support video functions, voice calls, or data transfer
  + Broadcast traffic for network operations
  + Multicast traffic for real-time media streams

All these can be business-critical traffic; however, you need to prioritize them to eliminate network congestion. Network devices treat this intermixed traffic equally, which can cause network issues and outages. Organizations can use Quality of Service (QoS) protocols to manage misconfigured traffic.

* **Business – Critical Traffic:** In a business network, the network manager decides which type of network is business-critical to ensure the required bandwidth is reserved. The remaining bandwidth can be used for traffic coming from other sources.
* **Outdated or Non-Compatible Hardware:** Enterprises must look for outdated and non-compatible devices and try upgrading network capacity to speed up the enterprise's network demands. A hardware upgrade is critical to have an optimal layout. If hardware assets such as switches, routers, servers, and cable connections can’t handle the data speeds the network requires, they can slow down the network and lead to network congestion.
* **Overused and too many devices:** Overused devices can also contribute to network congestion. Pushing devices to their maximum capacity can often result in over-utilization. Excessive volumes of device usage can also cause network congestion as they can provide a surplus of requests for data.
* **Bandwidth hogs:** A bandwidth hog is the over-usage of data on a particular device. The difference between average data usage and a hog's usage depends on the user or device. It’s important to monitor bandwidth in real-time to detect a bandwidth hog.

**How to solve network congestion problems**

* Traffic and bandwidth monitoring: The first step to resolve network congestion is to identify issues such as over-utilization of devices, insufficient bandwidth, and more. Monitoring networks also provide sufficient insights to identify problematic areas. You can also use network performance monitoring tools to identify such issues quickly. Once you get insights into your network performance and how data traffic flows, you can upgrade your devices, bandwidth, or network hardware to maximize the benefit.
* Segmenting and prioritizing: Segmenting your network into small subnets increases efficiency by letting you prioritize traffic. This also helps you accurately monitor network traffic. Segmenting networks can reduce data traffic, producing a more viable network. Prioritization refers to the capacity to minimize traffic. Critical network traffic areas need more attention than others.

**Helpful tools for monitoring and preventing network congestion**

Several network performance monitoring tools can detect bandwidth hogs and monitor network traffic to help ensure there is no congestion. These tools help to:

* Monitor and analyze network traffic patterns down to the interface level and help IT teams identify endpoints, protocols, and applications that consume more bandwidth.
* Create reports to analyze and monitor network bandwidth more precisely. These tools convert raw numbers into easy-to-interpret charts, tables, and utilization reports to better understand how the network is being used.
* Get instant alerts, so you can quickly act if traffic increases or decreases and efficiently remediate the problem.

Congestion Control Algorithms

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

**Effects** of Congestion

* As delay increases, performance decreases.
* If delay increases, retransmission occurs, making situation worse.

**Congestion control algorithms**

* Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
* Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

There are two congestion control algorithm which are as follows:

1. **Leaky Bucket Algorithm**

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.

* A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
* This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
* The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
* The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.

[](https://media.geeksforgeeks.org/wp-content/uploads/leaky.jpg)

Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

* When host wants to send packet, packet is thrown into the bucket.
* The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
* Bursty traffic is converted to a uniform traffic by the leaky bucket.
* In practice the bucket is a finite queue that outputs at a finite rate.

**Token bucket Algorithm**

* The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
* In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
* It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
* The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
* When tokens are shown, a flow to transmit traffic appears in the display of tokens.
* No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

**Need** of token **bucket Algorithm**:-

 The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

**Steps** of this algorithm can be described as follows:

* In regular intervals tokens are thrown into the bucket. ƒ
* The bucket has a maximum capacity. ƒ
* If there is a ready packet, a token is removed from the bucket, and the packet is sent.
* If there is no token in the bucket, the packet cannot be sent.

**Example**

 In figure

1. We see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token.
2. We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

**Ways in which token bucket is superior to leaky bucket:** The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

**Formula:**

M \* s = C + ρ \* s

Where

S – is time taken

M – Maximum output rate

ρ – Token arrival rate

C – Capacity of the token bucket in byte

Let’s understand with an example,

[](https://media.geeksforgeeks.org/wp-content/uploads/leakybuk.jpg)

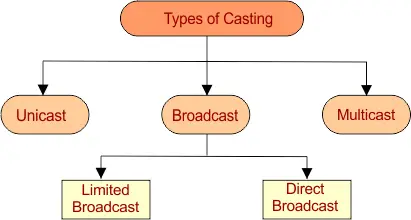
Network Layer in the Internet

**Casting and Its Types**

Casting is a method of transferring a packet to various hosts simultaneously by using an IP address.

**Types of Casting**

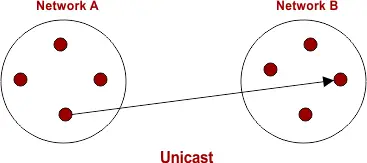
There are three types of casting



**1) Unicast**

Transmitting a packet from one source node to one destination node is called as unicast.

We can say, it is a one to one transmission.



**Example**

Consider a Node/Host “A” having IP Address 11.2.2.31 in one network is sending data to Node/Host “B” having IP Address 21.11.41.21 in another network.

Then,

Source IP Address of Host A = 11.2.2.31

Destination IP Address of Host B = 21.11.41.21.

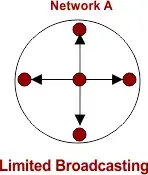
**2) Broadcast**

* In Broadcasting, Packet is send to all residing host in the same or different network, depending on its types.
* It is a one to all transmission.

Broadcasting is of two types

1. Limited Broadcast
2. Direct Broadcast
3. **Limited Broadcast**

According to Limited Broadcasting, Packet is send to all residing host in the same network



* If a Host need to send a broadcast message with in the same network then All 32 bits of IP address are set to 1. As
* Limited Broadcast Address for any network = 11111111.11111111.11111111.11111111 = 255.255.255.255
* This IP address cannot pass through router to go for another network.

**Example**

Consider a Node/Host “A” having IP Address 11.2.2.31 is sending data to all other hosts residing in the same network.

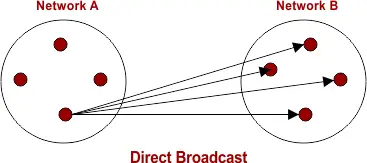
Then,

Source IP Address = IP Address of host A = 11.2.2.31

Destination IP Address = 255.255.255.255

**b) Direct Broadcast**

According to Limited Broadcasting, Packet is send to all residing host in the other network



* If a Host in a network wants to send a broadcast message to other network then all hosts bits of IP address are set to 1.
* This IP address cannot pass through router to go for another network.

**Example**

Host “A” in one Network having IP Address 11.11.121.13 sending data to all other hosts residing in the network having IP Address 21.0.0.0

Then,

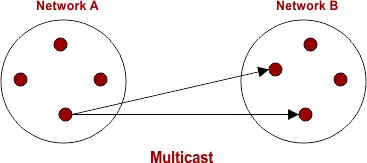
Source IP Address of host A = 11.11.121.13

Destination Address = 21.255.255.255

**3) Multicast**

Transmitting data packet from one source Node to a particular group of Nodes is known as Multicast.

It is also an example of one to many transmission.



**Examples**

Sending a message to group of people on whatsapp.

Video conference to a particular group of people

Note: To identify the group in multicast, IGMP (Internet Group Management Protocol) is used.

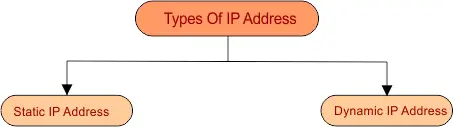
**IP Address in Networking**

In computer networking IP addressing is used at network layer,

* IP stand for Internet Protocol.
* IP address is a unique address which is assigned by ISP to each device whenever it connected to internet.

**Types of IP Address**

There are two types of IP address



**1) Static IP Address**

After assigning a Static IP Addresses to host, it always remains the They are configured manually.

**Note:**Some internet service providers (ISPs) do not provide static IP addresses. Static IP are more costly than dynamic IP Addresses.

**2) Dynamic IP Address**

* Dynamic IP Address is a temporarily assigned IP Address to any host of a network. It can be assigned to a different device if it is available (not in use of any Host).
* DHCP (Dynamic Host Configuration Protocol) or PPPoE (point to point connection over Ethernet) assigns dynamic IP addresses.

**IP Address Versions**

IP address is classified into two versions



IPv4 is mostly using now a days. However both IPv4 and IPv6 are supported by mostly Operating systems and manufacturer of networking devices.

**IPv4 Address Format**

* IPv4 Address is a 32 bit binary address which has 4 octet. Each octet (8-bits) are separated by dot (“.”).
* it supports 232 or 4.3 billion IP addresses. IPv4 addresses are not enough due to  rapid growth of internet.
* In IPv4, Some octets are fixed for Net ID and rest of octet are reserve for Host ID.



**NET ID:** Net ID always contains the some first octets out of 4 octets. Net ID is used to identify the network in which Host/computer exists.

**Host ID:** Host section always contains the least octet of IP address. It identifies the actual Host/computer in the network.

So, IP address (Network ID and Host ID) represents the location of host in the network.

**IPv4 Address Example**

Example of an IP Address in Binary = 00000011.10100001.00001011.11110001

Example of an IP Address in Binary Decimal Representation = 3.161.11.241

**IPv6 Address Format**

As the IPv4 are running out as with the growing of internet. And IPv6 comes into picture, it use 128-bit address techniques as compared to 32-bit IPv4. IPv6 provides (2128) unique IP addresses.

**IPv6 Address Example**

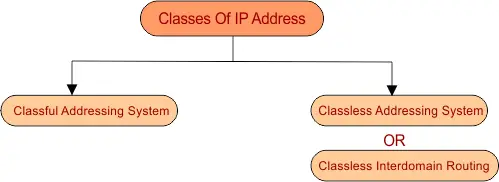
It is doted in hexadecimal instead of decimal, as given below

6789.ABCD.1234.EF92. 6789.ABCD.1234.EF92

Each hexadecimal character is denoted by 4 binary bits.  IPv6 may also be unicast, multicast or broadcast.

**IP Addressing**

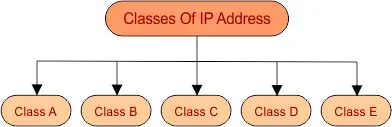
IP addressing is classified into two systems which are



In the upcoming lecture we will learn Classful and classless IP addressing.

**Classful IP Addressing**

In classful IP addressing, there are five classes which are given below



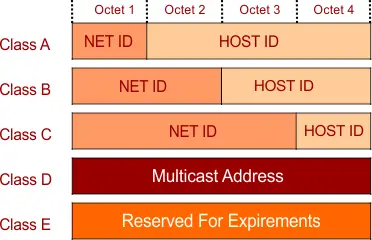
**In each class, two hosts IP are reserved**

* First host-IP in the network which is zero (i.e. for class A (1.0.0.0) represents to that network and cannot be assign to any host in the network.
* And last IP in the network (i.e. for class A (126.255.255.255) used for broadcasting.

**In each class, Some Leading Bits are reserved For Class Identification**

* For class A, The first one leading bit is always fix to “0”
* For class B, The first two leading bits are always fixed to “10”
* For class C, The first three leading bits are always fixed to “110”
* For class D, The first four leading bits are always fixed to “1110”
* For class E, The first four leading bits are always fixed to “1111”

Look at the following diagram for batter understanding



Number of networks and number of hosts in each class can be calculated through the following formula



Important To find Subnet mask of each class, Replace all Host octets to Zero and Network Octets to 255.

**Class A**

* First octet (8-bits) represent network ID and remaining 3-octet (24-bits) represents the host ID. The first 1 leading bit of network ID in Class A is always (0) and remaining 7-bits represent network ID.
* Format: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH (in binary)



* Start to End IP Address = (0.0.0.0 to 127.255.255.255)
* Value of first octet = 0 – 127
* Possible network ID’s = (27) = 128

**Important Note:**In class A, Network ID Zero (i.e. 0.0.0.0)  is reserved for default network and Network ID 127 (i.e. 127.0.0.0) is reserved for loopback (used for software testing). So, the remaining 126 (1-126) networks ID’s are used in class A.

* Possible Hosts = (224-2) = 16777214
* Total number of possible IP addresses = (231) = 2,147,483,648 (because “1 out of 32” bit is leading bit)
* First IP address = 0.0.0.0
* First Host address = 0.0.0.1
* Last IP address = 127.255.255.255
* Last Host address = 127.255.255.254
* Subnet Mask = 255.0.0.0

**Example**

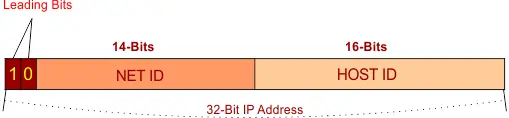


**Note:**Class A Network is used for large size companies because it has large number of hosts.

**Class B**

First two octets (16-bits) represent network ID and remaining 2-octets (16-bits) represents the host ID. The first two leading bit of network ID in Class B are always (10) and remaining 14-bits represent network ID.

* Format: 10NNNNNN. NNNNNNNN.HHHHHHHH.HHHHHHHH (in binary)



* Start to End Address IP addresses = (128.0.0.0 to 191.255.255.255)
* Value of first octet = (10000000 – 10111111) = 128 – 191
* Possible network ID = (214) = 16384
* Possible Hosts = (216-2) = 65534
* Possible Total number of IP addresses = (230) = (2 out of 32 bit is leading bit)
* First IP address = 128.0.0.0
* First Host address = 128.0.0.1
* Last IP address = 191.255.255.255
* Last Host address = 191.255.255.254
* Subnet Mask = 255.255.0.0

**Example:**

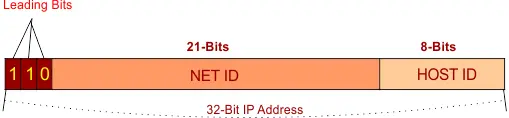


**Note:**Class B Network is used for medium size companies because it has small number of hosts as compare to class A.

**Class C**

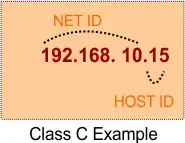
First three octets (24-bits) represent network ID and remaining 1-octet (8-bits) represents the host ID. The first three leading bit of network ID in Class B are always (110) and remaining 21-bits  represent network ID.

* Format: 110NNNNN. NNNNNNNN. NNNNNNNN.HHHHHHHH (in binary)



* Start to End Address IP addresses = (192.0.0.0 to 223.255.255.255) (in hexadecimal)
* Value of first octet = (11000000 – 11011111) = 192 – 223
* Possible network ID = (221) = 2097152
* Possible Hosts = (28-2) = 254
* Possible Total number of IP addresses = (229) = (3 out of 32 bit is leading bit)
* First IP address =192.0.0.0
* First Host address = 192.0.0.1
* Last IP address = 223.255.255.255
* Last Host address = 223.255.255.254
* Subnet Mask = 255.255.2555.0

**Example:**



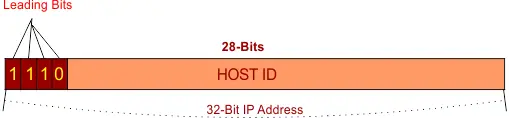
**Note:**Class C Network is used for small size companies because it has small number of hosts as compare to class A and B.

**Class D**

Class D is used for multicasts. Multicasting is used to pass the copies of datagram to selected groups of hosts instead of individual host. Class D is slightly different class from first three classes.

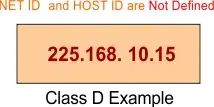
The first four leading bit of network ID in Class D are always (1110) and remaining 28-bits  represent group of computers where the multicast message will be passed.

* Format: 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm (in binary)



* Start to End Address IP addresses = (224.0.0.0 to 247.255.255.255) (in hexadecimal)
* Value of first octet = (11100000 – 11101111) = 224 – 247
* Possible Total number of IP addresses = (228) = (4 out of 32 bit is leading bit)
* First IP address = 224.0.0.0
* First Host address = 224.0.0.1
* Last IP address = 239.255.255.255
* Last Host address = 223.255.255.254
* **Subnet Mask, Network ID and Host ID are not defined in Class D**

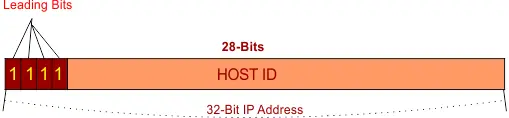
**Example**



**Class E**

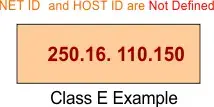
Class E is used for future Experimental purpose only. It is mostly used in research and development fields.  The first four leading bit of network ID in Class E are always (1111)

* Format: 1111rrrr. rrrrrrrr. rrrrrrrr. rrrrrrrr (in binary)

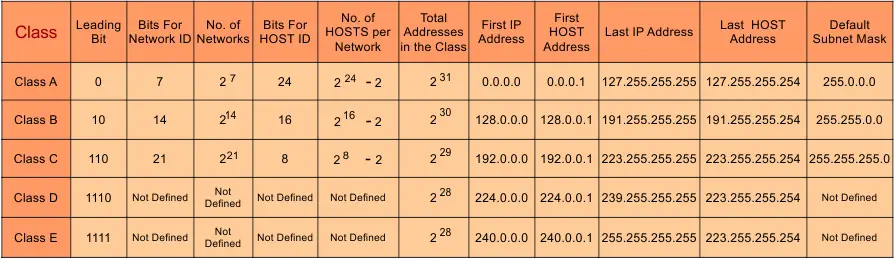


* Start to End Address IP addresses = (248.0.0.0 to 255.255.255.255) (in hexadecimal)
* Value of first octet = (11110000 – 11111111) = 248 – 255)
* Possible Total number of IP addresses = (228) = (4 out of 32 bit is leading bit)
* First IP address = 240.0.0.0
* First Host address = 240.0.0.1
* Last IP address = 255.255.255.255
* Last Host address = 223.255.255.254
* **Subnet Mask, Network ID and Host ID are not defined in Class E**

**Example:**



**Descriptive diagram of IP Classes**



IP PROTOCOL

An Internet Protocol (IP) address is a unique numerical identifier for every device or network that connects to the internet. Typically assigned by an internet service provider (ISP), an IP address is an online device address used for communicating across the internet.

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

What is an IP Address?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

Watch this video to learn what IP address is, why IP address is important and how to protect it from hackers:

**How do IP addresses work?**

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working, it helps understand how IP addresses work.

Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The use of IP addresses typically happens behind the scenes. The process works like this:

1. Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.
2. When you are ~~at~~ home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.
3. Your IP address is assigned to your device by your ISP.
4. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
5. However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.
6. When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

As the process implies, there are different types of IP addresses, which we explore below.

**Types of IP addresses**

There are different categories of IP addresses, and within each category, different types.

1. **Consumer IP addresses:** Every individual or business with an internet service plan ~~will~~ have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.
2. **Private IP addresses:** Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.
3. **Public IP addresses:** A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.
4. **Public IP addresses:** Public IP addresses come in two forms – dynamic and static.
   1. **Dynamic IP addresses:** Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don’t have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.
   2. **Static IP addresses:** In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

**Two types of website IP addresses.**

For website owners who don’t host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

1. **Shared IP addresses:** Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.
2. **Dedicated IP addresses:** Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

**How to look up IP addresses**

The simplest way to check your router’s public IP address is to search “What is my IP address?” on Google. Google will show you the answer at the top of the page.

Other websites will show you the same information: they can see your public IP address because, by visiting the site, your router has made a request and therefore revealed the information. The site IP Location goes further by showing the name of your ISP and your city.

Generally, you will only receive an approximation of location using this technique — where the provider is, but not the actual device location. If you are doing this, remember to log out of your VPN too. Obtaining the actual physical location address for the public IP address usually requires a search warrant to be submitted to the ISP.

Finding your private IP address varies by platform:

* **In Windows:**
  + Use the command prompt.
  + Search for “cmd” (without the quotes) using Windows search
  + In the resulting pop-up box, type “ipconfig” (no quote marks) to find the information.
* **On a Mac:**
  + Go to System Preferences
  + Select network – and the information should be visible.
* **On an iPhone:**
  + Go to Settings
  + Select Wi-Fi and click the “i" in a circle () next to the network you are on – the IP address should be visible under the DHCP tab.

If you need to check the IP addresses of other devices on your network, go into the router. How you access the router depends on the brand and the software it uses. Generally, you should be able to type the router's gateway IP address into a web browser on the same network to access it. From there, you will need to navigate to something like "attached devices," which should display a list of all the devices currently or recently attached to the network — including their IP addresses.

**IP address security threats**

Cybercriminals can use various techniques to obtain your IP address. Two of the most common are social engineering and online stalking.

Attackers can use social engineering to deceive you into revealing your IP address. For example, they can find you through Skype or a similar instant messaging application, which uses IP addresses to communicate. If you chat with strangers using these apps, it is important to note that they can see your IP address. Attackers can use a Skype Resolver tool, where they can find your IP address from your username.

**Online stalking:** Criminals can track down your IP address by merely stalking your online activity. Any number of online activities can reveal your IP address, from playing video games to commenting on websites and forums.

Once they have your IP address, attackers can go to an IP address tracking website, such as whatismyipaddress.com, type it in, and then get an idea of your location. They can then cross-reference other open-source data if they want to validate whether the IP address is associated with you specifically. They can then use LinkedIn, Facebook, or other social networks that show where you live, and then see if that matches the area given.

If a Facebook stalker uses a [phishing](https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips) attack against people with your name to install spying malware, the IP address associated with your system would likely confirm your identity to the stalker.

If cybercriminals know your IP address, they can launch attacks against you or even impersonate you. It is important to be aware of the risks and how to mitigate them. Risks include:

**Downloading illegal content using your IP address:** Hackers are known to use hacked IP addresses to download illegal content and anything else they do not want to be traced back to them. For example, using the identity of your IP address, criminals could download pirated movies, music, and video – which would breach your ISP’s terms of use – and much more seriously, content related to terrorism or child pornography. This could mean that you – through no fault of your own – could attract the attention of law enforcement.

**Tracking down your location:** If they know your IP address, hackers can use geolocation technology to identify your region, city, and state. They only need to do a little more digging on social media to identify your home and potentially burgle it when they know you are away.

**Directly attacking your network:** Criminals can directly target your network and launch a variety of assaults. One of the most popular is a DDoS attack (distributed denial-of-service). This type of cyberattack occurs when hackers use previously infected machines to generate a high volume of requests to flood the targeted system or server. This creates too much traffic for the server to handle, resulting in a disruption of services. Essentially, it shuts down your internet. While this attack is typically launched against businesses and video game services, it can occur against an individual, though this is much less common. Online gamers are at particularly high risk for this, as their screen is visible while streaming (on which an IP address can be discovered).

**Hacking into your device:** The internet uses ports as well as your IP address to connect. There are thousands of ports for every IP address, and a hacker who knows your IP can try those ports to attempt to force a connection. For example, they could take over your phone and steal your information. If a criminal does obtain access to your device, they could install malware on it.

**How to protect and hide your IP address**

Hiding your IP address is a way to protect your personal information and online identity. The two primary ways to hide your IP address are:

1. Using a proxy server
2. Using a virtual private network (VPN)

A **proxy server** is an intermediary server through which your traffic is routed:

* The internet servers you visit see only the IP address of that proxy server and not your IP address.
* When those servers send information back to you, it goes to the proxy server, which then routes it to you.

A drawback of proxy servers is that some of the services can spy on you — so you need to trust it. Depending on which one you use, they can also insert ads into your browser.

**VPN offers a better solution:**

* When you connect your computer – or smartphone or tablet – to a VPN, the device acts as if it is on the same local network as the VPN.
* All your network traffic is sent over a secure connection to the VPN.
* Because your computer behaves as if it is on the network, you can securely access local network resources even when you are in another country.
* You can also use the internet as if you were present at the VPN’s location, which has benefits if you are using public Wi-Fi or want to access geo-blocked websites.

Kaspersky Secure Connection is a VPN that protects you on public Wi-Fi, keeps your communications private, and ensures that you are not exposed to phishing, malware, viruses, and other cyber threats.

**When should you use VPN**

Using a VPN hides your IP address and redirects your traffic through a separate server, making it much safer for you online. Situations where you might use a VPN include:

**When using public Wi-Fi:** When using a public Wi-Fi network, even one that is password-protected, a VPN is advisable. If a hacker is on the same Wi-Fi network, it is easy for them to snoop on your data. The basic security that the average public Wi-Fi network employs does not provide robust protection from other users on the same network.

Using a VPN will add an extra layer of security to your data, ensuring you bypass the public Wi-Fi’s ISP and encrypting all your communication.

**When you are traveling:** If you are traveling to a foreign country – for example, China, where sites like Facebook are blocked – a VPN can help you access services that may not be available in that country.

The VPN will often allow you to use streaming services that you paid for and have access to in your home country, but they are not available in another because of international rights issues. Using a VPN can enable you to use the service as if you were at home. Travelers may also be able to find cheaper airfare when using a VPN, as prices can vary from region to region.

**When you are working remotely:** This is especially relevant in the post-COVID world, where many people are working remotely. Often employers require the use of a VPN to access company services remotely for security reasons. A VPN that connects to your office's server can give you access to internal company networks and resources when you are not in the office. It can do the same for your home network while you are out and about.

**When you just want some privacy:** Even in the comfort of your own home, using the internet for everyday purposes, using a VPN can be a good idea. Whenever you access a website, the server you connect to logs your IP address and attaches it to all the other data the site can learn about you: your browsing habits, what you click on, how long you spend looking at a particular page. They can sell this data to advertising companies who use it to tailor ads straight to you. This is why ads on the internet sometimes feel oddly personal: it’s because they are. Your IP address can also be used to track your location, even when your location services are turned off. Using a VPN prevents you from leaving footprints on the web.

Don’t forget your mobile devices, either. They have IP addresses too, and you probably use them in a wider variety of locations than your home computer, including public Wi-Fi hotspots. It is advisable to use a VPN on your mobile when connecting to a network you may not fully trust.

**Other ways to protect your privacy**

Apps installed on your device are a major source of IP address hacking. Instant messaging and other calling apps can be used as a tool by cybercriminals. Using IM apps only allows direct connections from contacts and doesn't accept calls or messages from people you don’t know. Changing your privacy settings makes it harder to find your IP address because people who don’t know you cannot connect with you.

**Create unique passwords**

Your device password is the only barrier that can restrict people from accessing your device. Some people prefer to stick to their devices' default passwords, which makes them vulnerable to attack. Like all your accounts, your device needs to have a unique and strong password that is not easy to decode. A strong password contains a mix of upper- and lower-case letters, numerals, and characters. This will help to safeguard your device against IP address hacking.

**Stay alert to phishing emails and malicious content**

A high proportion of malware and device tracking software is installed via phishing emails. When you connect with any site, this provides the site with access to your IP address and device location, making it vulnerable to hacking. Be vigilant when opening emails from unknown senders and avoid clicking on links that could send you to unauthorized sites. Pay close attention to the emails' content, even if they appear to come from well-known sites and legitimate businesses.

**Use a good antivirus solution and keep it up to date**

Install comprehensive antivirus software and keep it up to date. For example, Kaspersky’s Anti-Virus protection guards you from viruses on your PC and Android devices, secures and stores your passwords and private documents, and encrypts the data you send and receive online with VPN.

Protecting your IP address is a crucial aspect of protecting your online identity. Securing it through these steps is a way to stay safe against the wide variety of cybercriminals' attacks.

**IP ADDRESS**

**IPv4**

**IP** stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.   
IP version four addresses are 32-bit integers which will be expressed in decimal notation.   
**Example**- 192.0.2.126 could be an IPv4 address.

**Parts of IPv4**

**Network part:** The network part indicates the distinctive variety that’s appointed to the network. The network part conjointly identifies the category of the network that’s assigned.

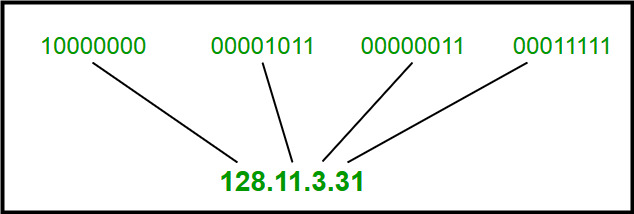
**Host Part:** The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.

For each host on the network, the network part is the same, however, the host half must vary.

**Subnet number:** This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

**IPv4 Address Format**

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).



**Characteristics of IPv4**

* IPv4 could be a 32-Bit IP Address.
* IPv4 could be a numeric address, and its bits are separated by a dot.
* The number of header fields is twelve and the length of the header field is twenty.
* It has Unicast, broadcast, and multicast style of addresses.
* IPv4 supports VLSM (Virtual Length Subnet Mask).
* IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
* RIP may be a routing protocol supported by the routed daemon.
* Networks ought to be designed either manually or with DHCP.
* Packet fragmentation permits from routers and causing host.

**Advantages of IPv4**

* IPv4 security permits encryption to keep up privacy and security.
* IPV4 network allocation is significant and presently has quite 85000 practical routers.
* It becomes easy to attach multiple devices across an outsized network while not NAT.
* This is a model of communication so provides quality service also as economical knowledge transfer.
* IPV4 addresses are redefined and permit flawless encoding.
* Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
* Data communication across the network becomes a lot of specific in multicast organizations.
* Limits net growth for existing users and hinders the use of the net for brand new users.
* Internet Routing is inefficient in IPv4.
* IPv4 has high System Management prices and it’s labor-intensive, complex, slow & frequent to errors.
* Security features are nonobligatory.
* Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

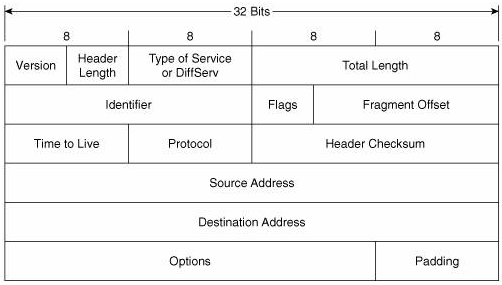
**Limitations of IPv4**

* IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
* The world’s supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
* If there are multiple host, we need IP addresses of next class.
* Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that’s why IPv6 came into the picture.

IPv4 Header

**Internet Protocol version 4** (**IPv4**) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet

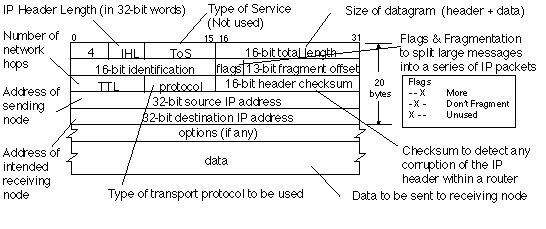
IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol , such as the Transmission Control Protocol (TCP).

**[](https://advancedinternettechnologies.files.wordpress.com/2012/01/ipv4-header.png)**

IPv4 Header

**The IPv4 packet header** consists of 14 fields, of which 13 are required. The 14th field is optional named: options. The IPv4 packet header consists of 20 bytes of data.

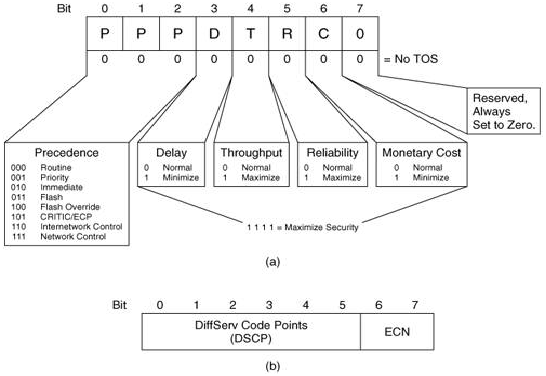
**Version**: The first header field in an IP packet is the four-bit version field. The Version field indicates the format of the internet header. Version identifies the IP version to which the packet belongs. This four-bit field is set to binary 0100 to indicate version 4 (IPv4) or binary 0110 to indicate version 6 (IPv6).

[](https://advancedinternettechnologies.files.wordpress.com/2012/01/untitled.png)

**Header length or Internet Header Length (IHL) :-** The second field (4 bits) is the Internet Header Length (IHL) telling the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum value for this field is 5 , which is a length of 5×32 = 160 bits = 20 bytes. Being a 4-bit value, the maximum length is 15 words (15×32 bits) or 480 bits = 60 bytes.

**Type of Service (ToS):–**now known as**Differentiated Services Code Point (DSCP).** The TOS field is used to carry information to provide quality of service features. New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

TOS allows the selection of a delivery service in terms of precedence, throughput, delay, reliability, and monetary cost.

[](https://advancedinternettechnologies.files.wordpress.com/2012/01/untitled1.png)

**Fig:-(a) Type of Service    and     (b) DSCP & ECN**

* **Explicit Congestion Notification (ECN) :-It**allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.
* **Total Length:-** This 16-bit field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes — the maximum value of a 16-bit word. The minimum size datagram that any host is required to be able to handle is 576 bytes, but most modern hosts handle much larger packets. Sometimes subnetworks impose further restrictions on the size, in which case datagrams must be fragmented. Fragmentation is handled in either the host or packet switch in IPv4.
* **Identification:–** This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.
* **Flags:–**A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):
* bit 0: Reserved; must be zero.
* bit 1: Don’t Fragment (DF)
* bit 2: More Fragments (MF)
* **Don’t Fragment:-**Sets the Don’t Fragment bit in sent packets. When an IP datagram has its DF flag set, intermediate devices are not allowed to fragment it so if it needs to travel across a network with a MTU(Maximum Transmission Unit) smaller that datagram length the datagram will have to be dropped. Normally an ICMP Destination Unreachable message is generated and sent back to the sender.
* **More Fragments:-**Sets the More Fragments bit in sent packets. The MF flag is set to indicate the receiver that the current datagram is a fragment of some larger datagram. When set to zero it indicates that the current datagram is either the last fragment in the set or that it is the only fragment.
* **Fragment Offset:-**The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of (213 – 1) × 8 = 65,528 bytes which would exceed the maximum IP packet length of 65,535 bytes with the header length included (65,528 + 20 = 65,548 bytes).
* **Time To Live (TTL):-**It is of 8 bit field. This field indicates the maximum time the datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it process the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime. *<hops>* must be a number in the range [0–255].
* **Protocol:-**This field defines the protocol used in the data portion of the IP datagram. The Internet Assigned Numbers Authority maintains a list of IP protocol numbers.
* **Header Checksum:-** The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded. Errors in the data field must be handled by the encapsulated protocol and both UDP and TCP have checksum fields.

*As the TTL field is decremented on each hop, a new checksum must be computed each time.*The checksum field is the 16-bit one’s complement of the one’s complement sum of all 16-bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

* **Source address:** Sets the source IP address. This option lets you specify a custom IP address to be used as source IP address in sent packets. This allows spoofing the sender of the packets. <addr> can be an IPv4 address or a hostname.
* **Destination address:** An IPv4 address indicating the receiver of the packet. As with the Source address, this may be changed in transit by a network address translation device.
* **Options:-**Additional header fields may follow the destination address field, but these are not often used. The value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header.

The option field is variable in length. There may be zero or more options. There are two cases for the format of an option:

**Case 1:** A single octet of option-type.

**Case 2:** An option-type octet, an option-length octet, and the actual option-data octets.

The option-length octet counts the option-type octet and the option-length octet as well as the option-data octets.

The option-type octet is viewed as having 3 fields:

1 bit copied flag,

2 bits option class,

5 bits option number.

The copied flag indicates that this option is copied into all fragments on fragmentation.

0 = not copied

1 = copied

The option classes are:

0 = control

1 = reserved for future use

2 = debugging and measurement

3 = reserved for future use

**Data**:- The data portion of the packet is not included in the packet checksum. Its contents are interpreted based on the value of the Protocol header field.

In a typical IP implementation, standard protocols such as TCP and UDP are implemented in the OS kernel for performance reasons. Other protocols such as ICMP may be partially implemented by the kernel, or implemented purely in user software.

**Some of the common protocols for the data portion are listed below:**

|  |  |  |
| --- | --- | --- |
| **Protocol number** | **Protocol name** | **Abbreviation** |
| 1 | Internet control message protocol | ICMP |
| 2 | Internet group management protocol | IGMP |
| 6 | Transmission control protocol | TCP |
| 17 | User Datagram protocol | UDP |
| 41 | IPv6 encapsulation | ENCAP |
| 89 | Open Shortest path first | OSPF |
| 132 | Stream Control Transmission Protocol | SCTP |

IPv6

IP address is your digital identity. It’s a network address for your computer so the Internet knows where to send you emails, data, etc.

IP address determines who and where you are in the network of billions of digital devices that are connected to the Internet.

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

The common type of IP address (is known as IPv4, for “version 4”). Here’s an example of what an IP address might look like: 25.59.209.224

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6, let’s see why? An IPv6 address consists of eight groups of four hexadecimal digits. Here’s an example IPv6 address:

3001:0da8:75a3:0000:0000:8a2e:0370:7334

This new IP address version is being deployed to fulfil the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

*IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456. To keep it straightforward, we will never run out of IP addresses again.*

**IPv6 Address Format**

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

ABCD : EF01 : 2345 : 6789 : ABCD : B201 : 5482 : D023

**<**================IPv6 Address Format **(**16 Bytes**)**============**>**

**Types of IPv6 Address**

Now that we know about what is IPv6 address let’s take a look at its different types.

1. **Unicast addresses** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
2. **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.
3. **Anycast addresses** It is assigned to a set of interfaces that typically belong to different nodes.

**Advantages of IPv6**

* **Reliability**
* **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
* **Stronger Security:** IP Security, which provides confidentiality, and data integrity, is embedded into IPv6.
* Routing efficiency
* Most importantly it’s the final solution for growing nodes in Global-network.

**Disadvantages of IPv6**

* **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
* **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

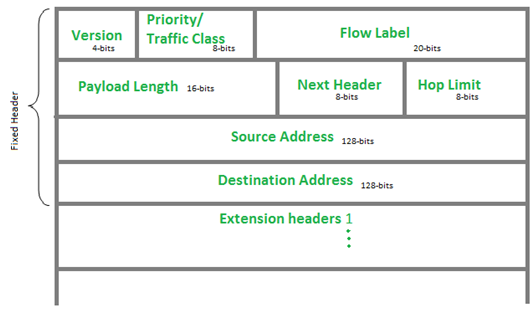
**Benefits of IPv6**

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

* **Larger Address Space:**IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
* **Improved Security:**IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more secure.
* **Simplified Header Format:**As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
* **Prioritize:**IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
* **Improved Support for Mobile Devices:**IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

Internet Protocol version 6 (IPv6) Header

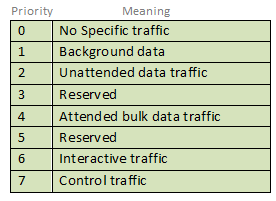
IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at the header of IP version 6 and understand how it is different from the IPv4 header.

**IP version 6 Header Format:**   


**Version (4-bits):**Indicates version of Internet Protocol which contains bit sequence 0110.

**Traffic Class (8-bits):**The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.

As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

Priority assignment of Congestion controlled traffic:   


Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to uncontrolled data traffic.

The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

**Flow Label (20-bits):**Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

**Payload Length (16-bits):**It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers (if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

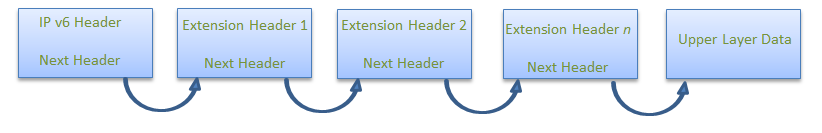
Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

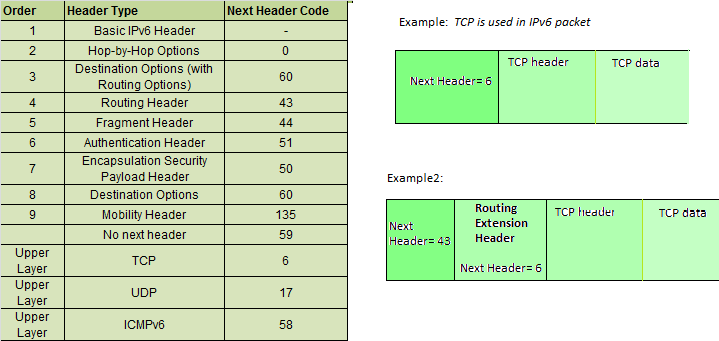
Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination (in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.



IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

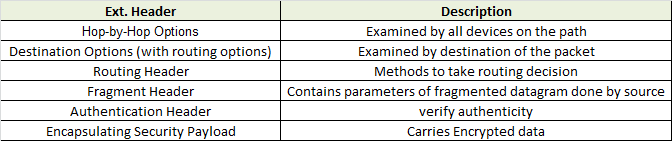


Rule: Hop-by-Hop options header (if present) should always be placed after the IPv6 base header. 

**Conventions**:

1. Any extension header can appear at most once except Destination Header because Destination Header is present two times in the above list itself.
2. If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in the routing header.
3. If Destination Header is present just above the Upper layer then it will be examined only by the Destination node.

Given order in which all extension header should be chained in IPv6 packet and working of each extension header:

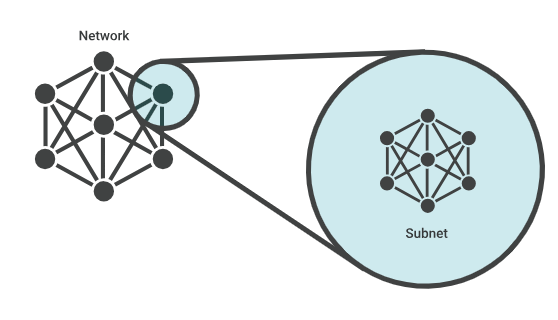


**Difference between IPv4 and IPv6**

| **IPv4** | **IPv6** |
| --- | --- |
| IPv4 has a 32-bit address length | IPv6 has a 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end-to-end, connection integrity is Achievable |
| It can generate 4.29×109 address space | The address space of IPv6 is quite large it can produce 3.4×1038 address space |
| The Security feature is dependent on the application | IPSEC is an inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation is performed only by the sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has a broadcast Message Transmission Scheme | In IPv6 multicast and anycast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has a header of 20-60 bytes. | IPv6 has a header of 40 bytes fixed |
| IPv4 can be converted to IPv6 | Not all IPv6 can be converted to IPv4 |
| IPv4 consists of 4 fields which are separated by addresses dot (.) | IPv6 consists of 8 fields, which are separated by a colon (:) |
| IPv4’s  IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E. | IPv6 does not have any classes of the IP address. |
| IPv4 supports VLSM(Variable Length subnet mask). | IPv6 does not support VLSM. |
| Example of IPv4:  66.94.29.13 | Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB |

SUBNETS

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

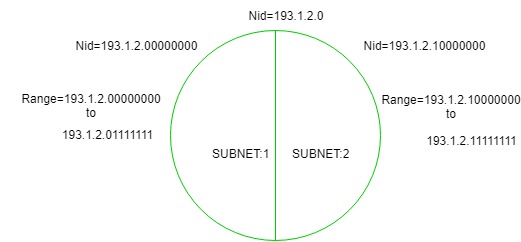


When a bigger network is divided into smaller networks, to maintain security, then that is known as **Subnetting**. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 224 for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

**Uses of Subnetting**

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing network security.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

**Note:** It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

**Subnetting Work**

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In class C the first 3 octets are network bits so it remains as it is.

* **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1’s in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet 1 is: **193.1.2.0 to 193.1.2.127**

Subnet id of Subnet-1 is : 193.1.2.0

The direct Broadcast id of Subnet-1 is: 193.1.2.127

The total number of hosts possible is: 126 (Out of 128,

2 id's are used for Subnet id & Direct Broadcast id)

The subnet mask of Subnet- 1 is: 255.255.255.128

* **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1’s in the host ID part i.e, 193.1.2.11111111).

Thus, the range of subnet-2 is: **193.1.2.128 to 193.1.2.255**

Subnet id of Subnet-2 is : 193.1.2.128

The direct Broadcast id of Subnet-2 is: 193.1.2.255

The total number of hosts possible is: 126 (Out of 128,

2 id's are used for Subnet id & Direct Broadcast id)

The subnet mask of Subnet- 2 is: 255.255.255.128

The best way to find out the subnet mask of a subnet

is to set the fixed bit of host-id to 1 and the rest to 0.

Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

**Note:**

1. To divide a network into four (22) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (23) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

Along with the advantage, there is a small disadvantage to subnetting that is, before subnetting to find the IP address first the network id is found then the host id followed by the process id, but after subnetting first network id is found then the subnet id then host id and finally process id by this the computation increases.

**Example 1:**An organization is assigned a class C network address of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

1. 201.35.2.129
2. 201.35.2.191
3. 201.35.2.255
4. Both (A) and (C)

**Solution:**

Converting the last octet of the

netmask into the binary form: 255.255.255.**11**000000

Converting the last octet of option 1

Into the binary form: 201.35.2.**10**000001

Converting the last octet of option 2

Into the binary form: 201.35.2.**10**111111

Converting the last octet of option 3

Into the binary form: 201.35.2.**11**111111

From the above, we see that Options 2 and 3 are not valid host IP addresses (as they are broadcast addresses of a subnetwork), and **OPTION 1** is not a broadcast address and it can be assigned to a host IP.

**Example 2:**An organization has a class C network address of 201.32.64.0. It uses a subnet mask of 255.255.255.248. Which of the following is NOT a valid broadcast address for any subnetworks?

1. 201.32.64.135
2. 201.32.64.240
3. 201.32.64.207
4. 201.32.64.231

**Solution:**

Converting the last octet of the netmask

into the binary form: 255.255.255.**11111**000

Converting the last octet of option 1

into the binary form: 201.32.64.**10000**111

Converting the last octet of option 2

into the binary form: 201.32.64.**11110**000

Converting the last octet of option 3

into the binary form: 201.32.64.**11001**111

Converting the last octet of option 4

into the binary form: 201.32.64.**11100**111

From the above, we can see that in OPTION 1, 3, and 4, all the host bits are 1 and give the valid broadcast address of subnetworks.

and **OPTION 2,** the last three bits of the Host address are not 1 therefore it’s not a valid broadcast address.

**Advantages of Subnetting**

The advantages of Subnetting are mentioned below:

* It provides security to one network from another network. eg) In an Organisation, the code of the Developer department must not be accessed by another department.
* It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department needs to host webcasts or video conferences.
* In the case of Small networks, maintenance is easy.

**Disadvantages of Subnetting**

The disadvantages of Subnetting are mentioned below:

* In the case of a single network, only three steps are required to reach a Process i.e Source Host to Destination Network, Destination Network to Destination Host, and then Destination Host to Process.
* In the case of a Single Network only two IP addresses are wasted to represent Network Id and Broadcast address but in the case of Subnetting two IP addresses are wasted for each Subnet.
* The cost of the overall Network also increases. Subnetting requires internal routers, Switches, Hubs, Bridges, etc. which are very costly.

INTERNET WORKING

**Introduction**

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, which function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it’s called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking. Internetworking is enforced in Layer three (Network Layer) of the OSI-ISO model. The foremost notable example of internetworking is the Internet.

There are chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn’t thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

1. **Extranet –** It’s a network of the internetwork that’s restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It’s the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. **Intranet –** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.
3. **Internet –** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the ‘Internet’ to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

Internetworking has evolved as an answer to a few key problems: isolated LANs, duplication of resources, and an absence of network management. Isolated LANs created transmission problems between totally different offices or departments. Duplication of resources meant that constant hardware and code had to be provided to every workplace or department, as did a separate support employee. This lack of network management meant that no centralized methodology of managing and troubleshooting networks existed.

One more form of the interconnection of networks usually happens among enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the amount of the TCP/IP logical interfaces. Such interconnection is accomplished through network bridges and network switches. This can be typically incorrectly termed internetworking, however, the ensuing system is just a bigger, single subnetwork, and no internetworking protocol, akin to web Protocol, is needed to traverse these devices.

However, one electronic network is also reborn into associate degree internetwork by dividing the network into phases and logically dividing the segment traffic with routers. The Internet Protocol is meant to supply an associate degree unreliable packet service across the network. The design avoids intermediate network components maintaining any state of the network. Instead, this task is allotted to the endpoints of every communication session. To transfer information correctly, applications should utilize associate degree applicable Transport Layer protocol, akin to Transmission management Protocol (TCP), that provides a reliable stream. Some applications use a less complicated, connection-less transport protocol, User Datagram Protocol (UDP), for tasks that don’t need reliable delivery of information or that need period of time service, akin to video streaming or voice chat.

**Internetwork Addressing –**

Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer. Three kinds of internetwork addresses area units are ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

1. **Data Link Layer addresses:** A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically area units cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre-established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.
2. **MAC Addresses:** Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area units distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, which are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses are typically area units referred to as burned-in addresses (BIAs) as a result of being burned into read-only memory (ROM) and are traced into random-access memory (RAM) once the interface card initializes.
3. **Network-Layer Addresses:** Network addresses sometimes exist among a gradable address area and typically area units referred to as virtual or logical addresses. the connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don’t have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

**Challenges to Internetworking –**

Implementing useful internetwork isn’t at any certainty. There are several challenging fields, particularly in the areas of dependableness, connectivity, network management, and adaptability, and each and every space is essential in establishing associate degree economical and effective internetwork. A few of them are:-

1. The initial challenge lies when we are trying to connect numerous systems to support communication between disparate technologies. For example, Totally different sites might use different kinds of media, or they could operate at variable speeds.
2. Another essential thought is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable access to network resources.
3. Network management should give centralized support associate degree troubleshooting capabilities on the internetwork. Configuration, security, performance, and different problems should be adequately addressed for the internetwork to perform swimmingly.
4. Flexibility, the ultimate concern, is important for network enlargement and new applications and services, among different factors.

#### Advantages:

1. **Increased connectivity: I**nternetworking enables devices on different networks to communicate with each other, which increases connectivity and enables new applications and services.
2. **Resource sharing:**Internetworking allows devices to share resources across networks, such as printers, servers, and storage devices. This can reduce costs and improve efficiency by allowing multiple devices to share resources.
3. **Improved scalability:**Internetworking allows networks to be expanded and scaled as needed to accommodate growing numbers of devices and users.
4. **Improved collaboration:** Internetworking enables teams and individuals to collaborate and work together more effectively, regardless of their physical location.
5. **Access to remote resources:**Internetworking allows users to access resources and services that are physically located on remote networks, improving accessibility and flexibility.

#### Disadvantages:

1. **Security risks:**Internetworking can create security vulnerabilities and increase the risk of cyberattacks and data breaches. Connecting multiple networks together increases the number of entry points for attackers, making it more difficult to secure the entire system.
2. **Complexity:**Internetworking can be complex and requires specialized knowledge and expertise to set up and maintain. This can increase costs and create additional maintenance overhead.
3. **Performance issues:**Internetworking can lead to performance issues, particularly if networks are not properly optimized and configured. This can result in slow response times and poor network performance.
4. **Compatibility issues:**Internetworking can lead to compatibility issues, particularly if different networks are using different protocols or technologies. This can make it difficult to integrate different systems and may require additional resources to resolve.
5. **Management overhead:**Internetworking can create additional management overhead, particularly if multiple networks are involved. This can increase costs and require additional resources to manage effectively.