UNIT – 3 : NETWORK LAYER

Introduction:

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

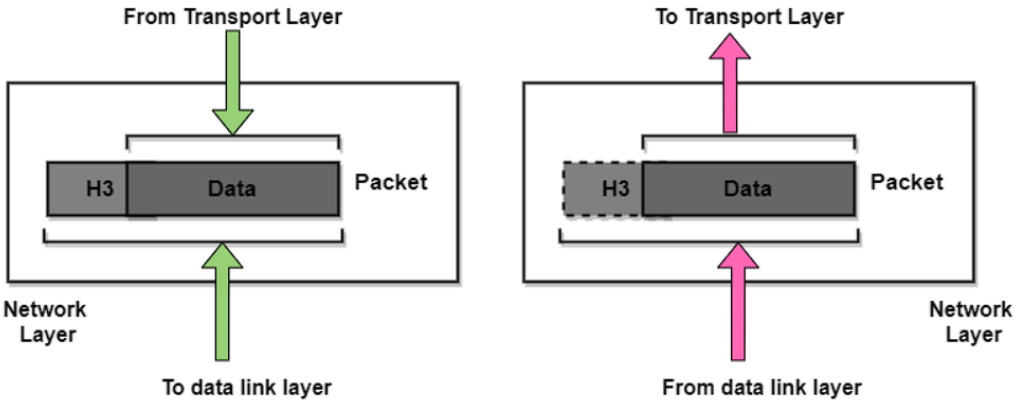


Figure: Network Layer

Functions of Network Layer:

The main functions performed by the network layer are:

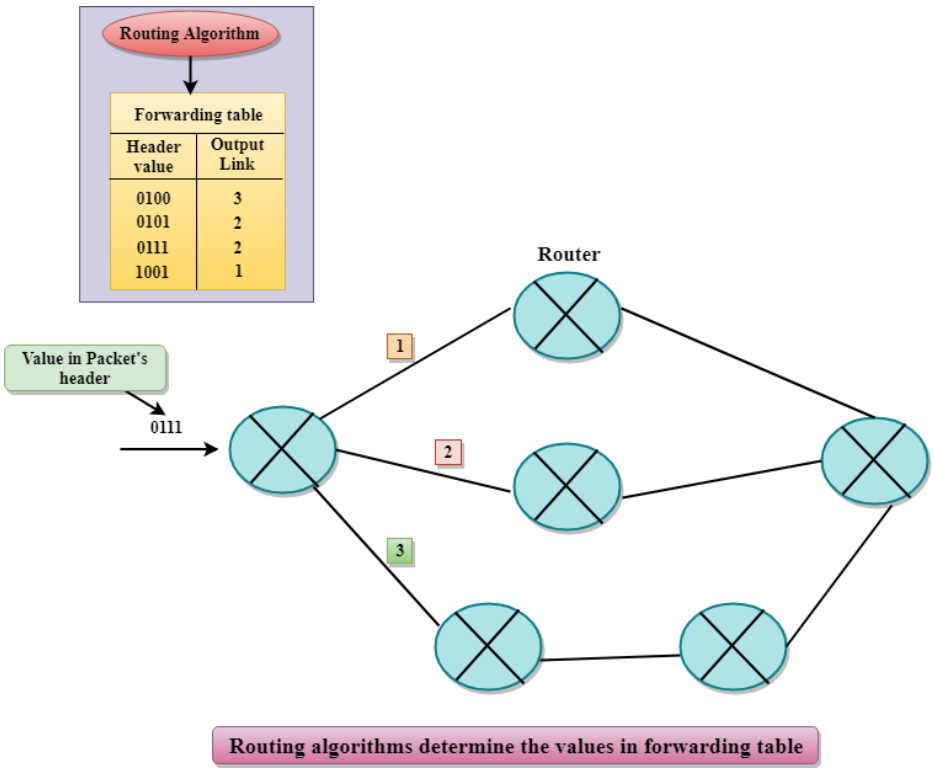
- **Host-to-host Data Delivery**: The network layer is responsible for delivering data packets from source to destination. This layer provides the service that ensures the packet will reach its intended destination.
- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.
- **Congestion Control:** When the data packets are flooded into the network in tremendous amounts, and the router is unable to route them properly, it causes aggregation of data packets into the network, which is referred to as congestion. The network layer is also responsible for controlling the congestion in the network and manipulating the flow of the network.

Forwarding & Routing:

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



Routing algorithms determine the values in forwarding table

Services Provided by the Network Layer:

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Advantages of Network Layer Services:

- Packetization service in the network layer provides ease of transportation of the data packets.
- Packetization also eliminates single points of failure in data communication systems.
- Routers present in the network layer reduce network traffic by creating collision and broadcast domains.
- With the help of Forwarding, data packets are transferred from one place to another in the network.

Disadvantages of Network Layer Services:

- There is a lack of flow control in the design of the network layer.
- Congestion occurs sometimes due to the presence of too many datagrams in a network that is beyond the capacity of the network or the routers. Due to this, some routers may drop some of the datagrams, and some important pieces of information may be lost.
- Although indirect error control is present in the network layer, there is a lack of proper error control mechanisms as due to the presence of fragmented data packets, error control becomes difficult to implement.

Design Issues:

Following are the Design Issues in Network Layer –

1. Store-and-Forward Packet Switching:

The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services Provided to Transport Layer:

The network layer provides services to the transport layer at the network layer/transport layer interface. The services need to be carefully designed with the following goals in mind:

1. The services should be independent of the router technology.

2. The transport layer should be shielded from the number, type, and topology of the routers present.

3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Based on the connections there are 2 types of services provided:

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:

Packet are termed as "**datagrams**" and corresponding subnet as "**datagram subnets**". 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 transmits each packet to router via. a few protocols. Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:

To use a connection-oriented service, first we establish a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

It can be done in either two ways:

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Comparison of Virtual-Circuit and Datagram Subnets:

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Routing:

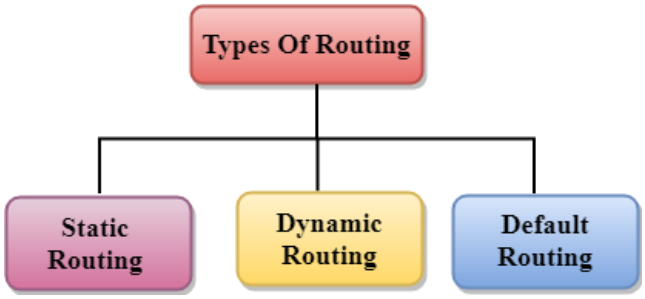
Routing is the process of choosing a path for traffic within a network and between or across networks. Routing is performed in many networks, including circuit-switched networks like the public switched telephone network (PSTN) and computer networks like the Internet. It is a process that uses layer 3 (or network layer) devices to deliver packets by selecting the best path from one network to another. The routing algorithm design and maintains the routing table for the path determination process.

In simple terms, suppose P1 is our network, and we want to send data to P2, and there are many networks between these two. Our network requires a router to choose the best path for our data to transfer from P1 to P2. The process of choosing the best path within or across networks for data exchange is known as Routing.

What is a Router?

A router is a piece of network hardware in charge of routing packets to their destinations. Routers connect to two or more IP networks or subnetworks and share the data packets as per the need. Routers are used in homes and offices to connect to local networks. We can find different kinds of routers based on their power found over the internet, which helps the data packets reach their destinations.

Classification of Routing:



1. Static Routing:

Another name for **Static Routing** is **Nonadaptive Routing**. Static routing is the process of manually joining routes to the routing table.

Let's suppose our computer wants to connect with another computer, and there are ten different networks between them. When we want to connect both the computers, we have to give the information manually about the networks through which we want to connect to the router, then only the exchange of data can be possible. This process is said to be Static Routing.

Advantages:

- The administrator manually sets it up.
- It is safe and quick.
- There is no bandwidth usage between routers.
- Because there is no routing overhead for the router CPU, a less expensive router can be used for routing.

Disadvantages:

- Utilized in small network
- Everything has to be set up manually.

2. Dynamic Routing:

Another name of **Dynamic Routing** is **Adaptive Routing**. Dynamic routing automatically adjusts routes based on the current state of the route in the routing table. Protocols are used in dynamic routing to discover network destinations and the routes that will take them there. The best examples of dynamic routing protocols are **RIP** and **OSPF**. If one of the network routes fails, it will make automatic adjustments to reach the network's destination.

Let's suppose our computer wants to connect with another computer. There are ten different networks between them, so the path they have to follow while connecting is chosen automatically, assuring security, collision, hacking, and many more.

Advantages:

- There is no need to understand the networks.
- Its setup is easy.
- Administrator work is less.
- It is used for big organizations.
- It is more effective at determining the best path in response to changes in the condition or topology.

Disadvantages:

- More bandwidth is consumed when interacting with other neighbours.
- Dynamic routing necessitates the use of more resources such as CPU, RAM, and bandwidth. That's why it's more expensive.
- Dynamic routing introduces more complexity to the network, especially during implementation.

3. Default Routing:

It is the method in which the router is set up to send all packets to a single router (next hop). It makes no difference to which network the packet belongs to; it is forwarded to the router that is set to default routing. It is typically used in conjunction with stub routers. A stub router only has one route to all other networks.

It is set up for unknown locations or end locations. It is the least preferred Routing. It helps in minimizing the size of your routing table.

Advantages:

- If there are no fixed routes in the routing table, the default route can be helpful. The default route is used for all packet traffic with an unknown destination in the routing table.
- It is suitable for packet filtering, firewalling, and proxy servers as it is configured for unknown destinations.

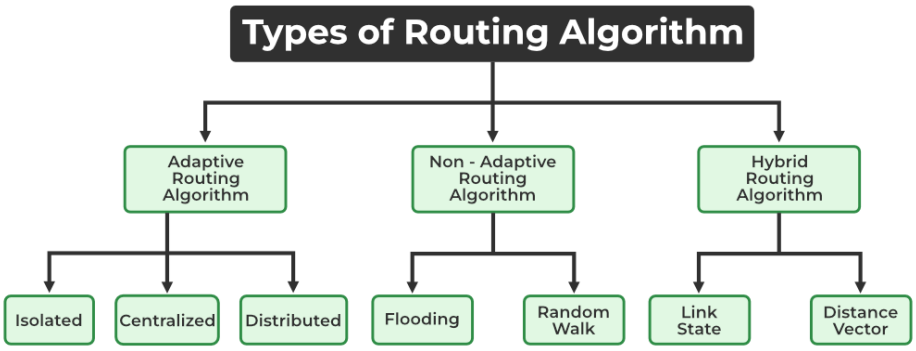
Disadvantages:

- If the network is overly complex, the setup will also be difficult.
- The network topology determines it.

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:



1. Adaptive Algorithms:

These are the algorithms that change their 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:

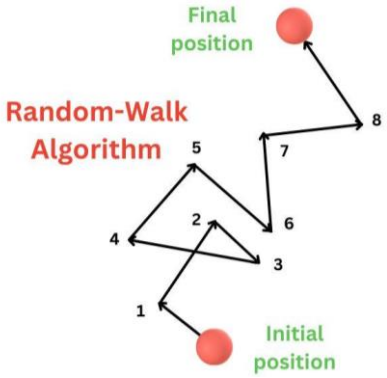
- **Isolated:** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes don't have information about the status of a particular link. The disadvantage is that packets may be sent through a congested network which 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.

2. 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** 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.



3. 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.

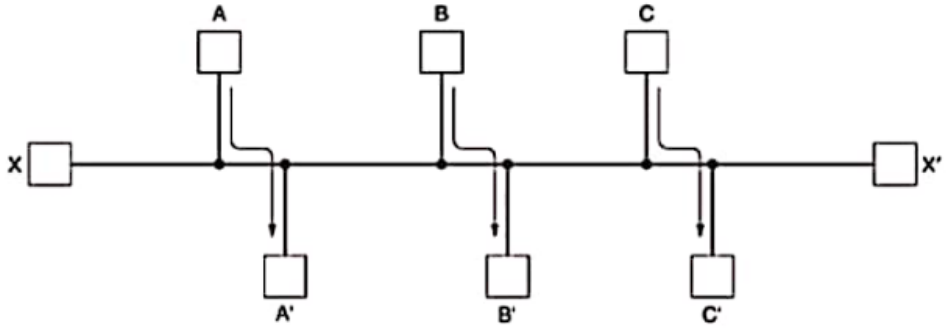
Differences b/w Adaptive and Non-Adaptive Routing Algorithm:

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non-Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

PROPERTIES OF ROUTING ALGORITHM:

Correctness, simplicity, robustness, stability, fairness, and optimality

FAIRNESS AND OPTIMALITY.



Fairness and optimality may sound obvious, but as it turns out, they are often contradictory goals. There is enough traffic between A and A', between B and B', and between C and C' to saturate the horizontal links. To maximize the total flow, the X to X' traffic should be shut off altogether. Unfortunately, X and X' may not see it that way. Evidently, some compromise between global efficiency and fairness to individual connections is needed.

Different Routing Algorithms:

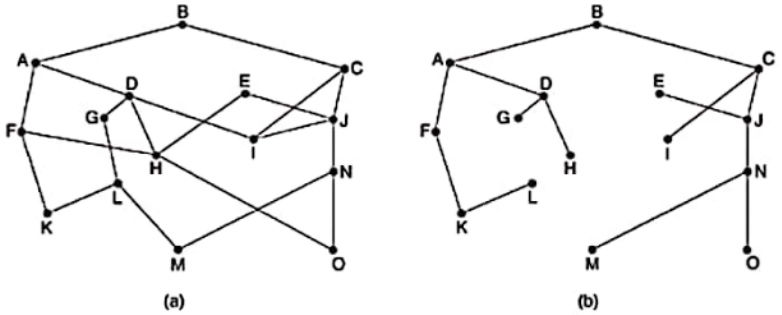
1. The Optimality Principle:

One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.

It states that "if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same."

As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree.

The goal of all routing algorithms is to discover and use the sink trees for all routers.



(a) A subnet. (b) A sink tree for router **B.**

2. Shortest Path Routing:

It refers to the algorithms that help to find the shortest path between a sender and receiver for routing the data packets through the network in terms of shortest distance, minimum cost, and minimum time.

- It is mainly for building a graph or subnet containing routers as nodes and edges as communication lines connecting the nodes.
- Hop count is one of the parameters that is used to measure the distance.
- **Hop count**: It is the number that indicates how many routers are covered. If the hop count is 6, there are 6 routers/nodes and the edges connecting them.
- Another metric is a geographic distance like kilometers.
- We can find the label on the arc as the function of bandwidth, average traffic, distance, communication cost, measured delay, mean queue length, etc.

Common Shortest Path Algorithms:

- Dijkstra's Algorithm
- Bellman Ford's Algorithm
- Floyd Warshall's Algorithm

Dijkstra's Algorithm:

The Dijkstra's Algorithm is a greedy algorithm that is used to find the minimum distance between a node and all other nodes in a given graph. Here we can consider node as a router and graph as a network. It uses weight of edge .ie, distance between the nodes to find a minimum distance route.

Algorithm:

1: Mark the source node current distance as 0 and all others as infinity.

2: Set the node with the smallest current distance among the non-visited nodes as the current node.

3: For each neighbor, N, of the current node:

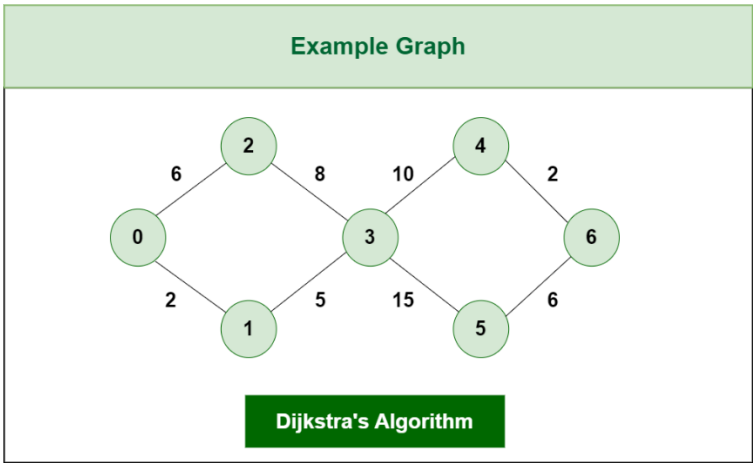
- Calculate the potential new distance by adding the current distance of the current node with the weight of the edge connecting the current node to N.
- If the potential new distance is smaller than the current distance of node N, update N's current distance with the new distance.

4: Make the current node as visited node.

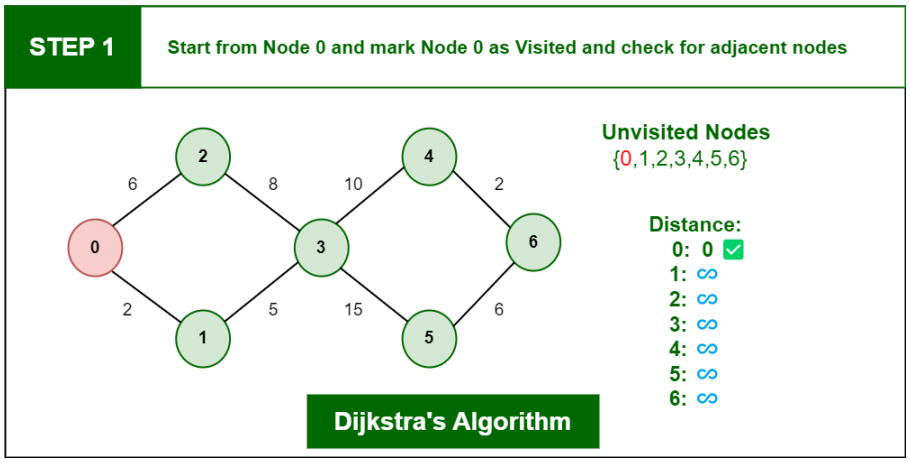
5: If we find any unvisited node, go to step 2 to find the next node which has the smallest current distance and continue this process.

Example:

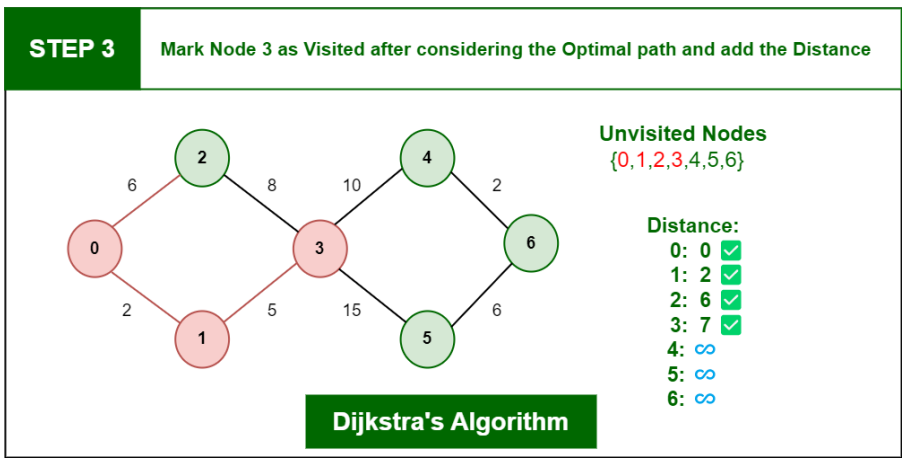
Consider the graph G:



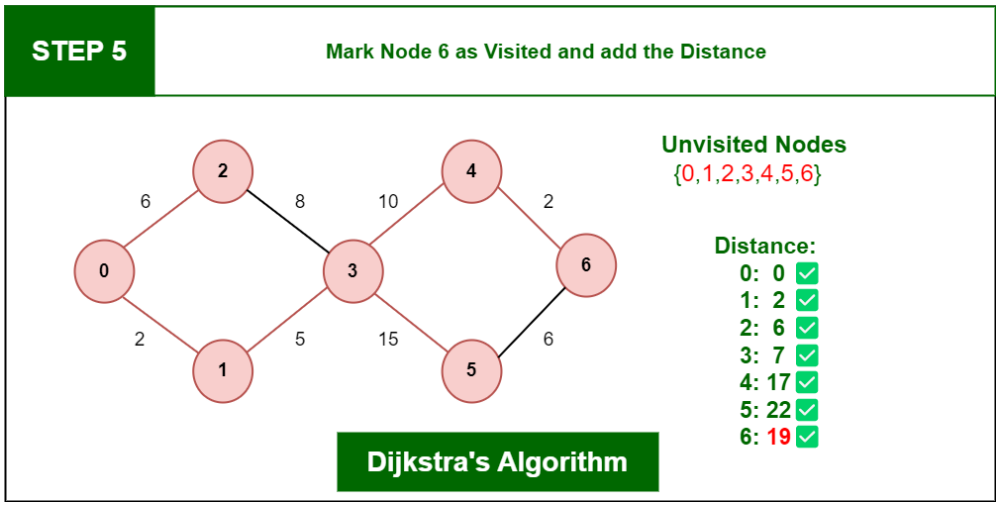
Now,we will start normalising graph one by one starting from node 0.



Nearest neighbour of 0 are 2 and 1 so we will normalize them first.



Similarly, we will normalize other node considering it should not form a cycle and will keep track in visited nodes.



Bellman Ford's Algorithm:

The Bell man Ford's algorithm is a single source graph search algorithm which help us to find the shortest path between a source vertex and any other vertex in a give graph. We can use it in both weighted and unweighted graphs. This algorithm is slower than Dijkstra's algorithm and it can also use negative edge weight.

Algorithm:

1: First we Initialize all vertices v in a distance array dist[] as INFINITY.

2: Then we pick a random vertex as vertex 0 and assign dist[0] =0.

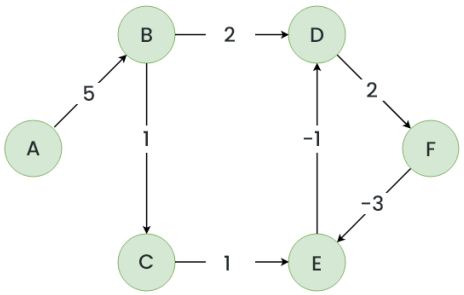
3: Then iteratively update the minimum distance to each node (dist[v]) by comparing it with the sum of the distance from the source node (dist[u]) and the edge weight (weight) N-1 times.

4: To identify the presence of negative edge cycles, with the help of following cases do one more round of edge relaxation.

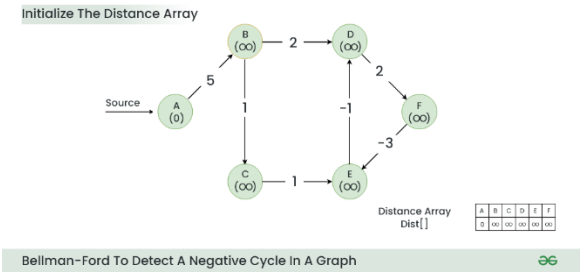
- We can say that a negative cycle exists if for any edge uv the sum of distance from the source node (dist[u]) and the edge weight (weight) is less than the current distance to the largest node(dist[v])
- It indicates the absence of negative edge cycle if none of the edges satisfies case1.

Example: Bellman ford detecting negative edge cycle in a graph.

Consider the Graph G:

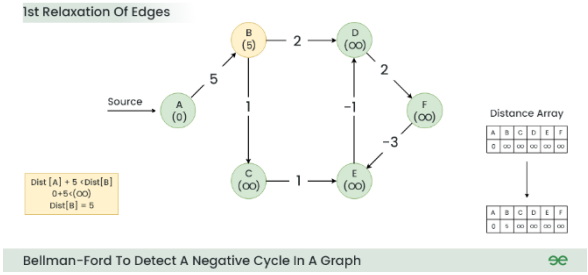


Bellman-Ford To Detect A Negative Cycle In A Graph



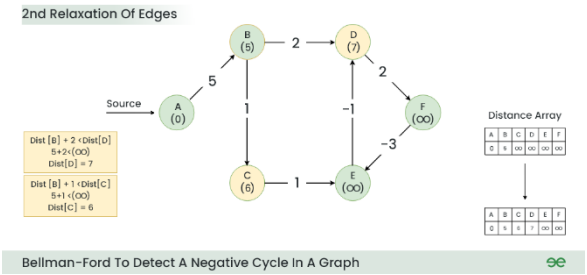
Bellman-Ford To Detect A Negative Cycle In A Graph

Step 1



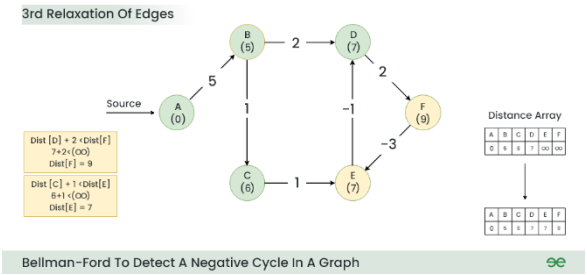
Bellman-Ford To Detect A Negative Cycle In A Graph

Step 2



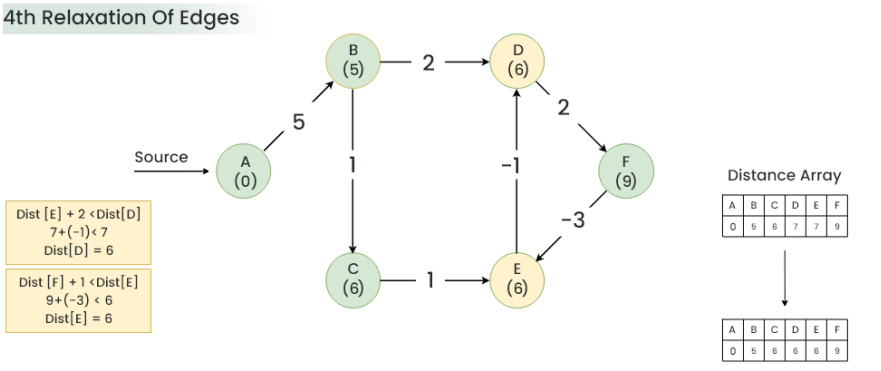
Bellman-Ford To Detect A Negative Cycle In A Graph

Step 3



Bellman-Ford To Detect A Negative Cycle In A Graph

Step 4



Bellman-Ford To Detect A Negative Cycle In A Graph

Step 5

Outcome: The graph contains a negative cycle in the path from node D to node F and then to node E.

Floyd Warshall's Algorithm:

The Floyd Warshall's Algorithm is used to find the shortest path between any two nodes in a given graph. It keeps a matrix of distances between each pair of vertices.it will continue iterating the matrix until it reaches at a shortest path.

Algorithm:

1: Using the data about the graph, make a matrix.

2: By taking all vertices as an intermediate vertex, we have to update the final matrix.

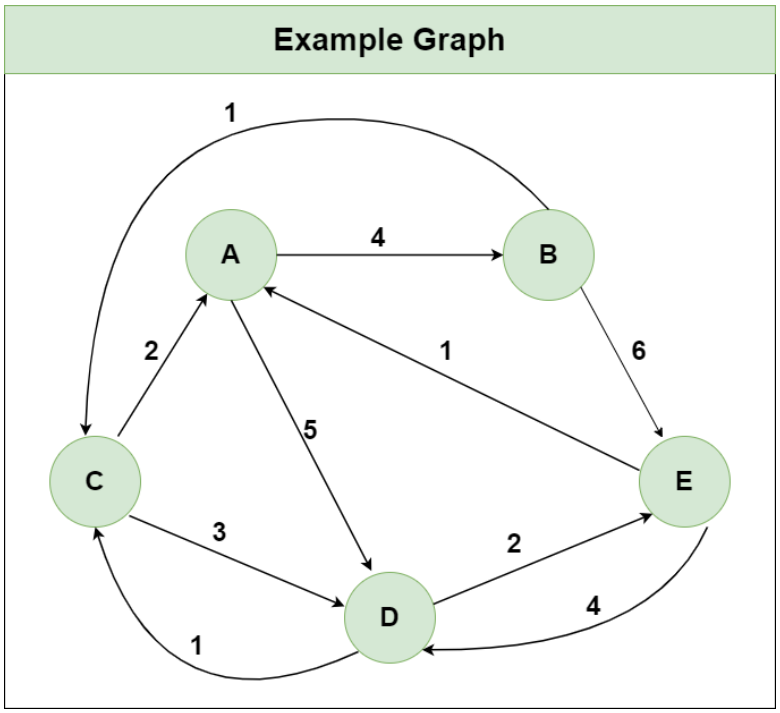
3: It is to be noted that it includes at a time we pick one vertex, and we update the shortest path which includes this chosen vertex as an in-between point along the path.

4: When we select a vertex say k almost like the middle of the path, in previous calculations we have already taken all vertices P{0,1,2..,k-1} as potential middle points.

5: We have to consider the following subpoints while dealing with the source and destination vertices I,j respectively

- If vertex k is not the part of shortest path from I to j, we don't have to change dist[i][j] value .ie, it will remain unchanged.
- If vertex k is indeed part of shortest path from I to j, update dist[i][j] to the sum of dist[i][k] and dist[k][j] but note that only if dist[i][j] is greater than this value we newly calculated.

Example: Consider the given graph G,



Step1: Initializing Distance[ ][ ] using the Input Graph

	A	B	C	D	E
A	0	4	∞	5	∞
B	∞	0	1	∞	6
C	2	∞	0	3	∞
D	∞	∞	1	0	2
E	1	∞	∞	4	0

Step 2: Using Node A as the Intermediate node

Distance[i][j] = min (Distance[i][j], Distance[i][A] + Distance[A][j])

	A	B	C	D	E
A	0	4	∞	5	∞
B	∞	?	?	?	?
C	2	?	?	?	?
D	∞	?	?	?	?
E	1	?	?	?	?

→

	A	B	C	D	E
A	0	4	∞	5	∞
B	∞	0	1	∞	6
C	2	6	0	3	12
D	∞	∞	1	0	2
E	1	5	∞	4	0

Step 3: Using Node B as the Intermediate node

Distance[i][j] = min (Distance[i][j], Distance[i][B] + Distance[B][j])

	A	B	C	D	E
A	?	4	?	?	?
B	∞	0	1	∞	6
C	?	6	?	?	?
D	?	∞	?	?	?
E	?	5	?	?	?

	A	B	C	D	E
A	0	4	5	5	10
B	∞	0	1	∞	6
C	2	6	0	3	12
D	∞	∞	1	0	2
E	1	5	6	4	0

Step 4: Using Node C as the Intermediate node

Distance[i][j] = min (Distance[i][j], Distance[i][C] + Distance[C][j])

	A	B	C	D	E
A	?	?	5	?	?
B	?	?	1	?	?
C	2	6	0	3	12
D	?	?	1	?	?
E	?	?	6	?	?

	A	B	C	D	E
A	0	4	5	5	10
B	3	0	1	4	6
C	2	6	0	3	12
D	3	7	1	0	2
E	1	5	6	4	0

Step 5: Using Node D as the Intermediate node

Distance[i][j] = min (Distance[i][j], Distance[i][D] + Distance[D][j])

	A	B	C	D	E
A	?	?	?	5	?
B	?	?	?	4	?
C	?	?	?	3	?
D	3	7	1	0	2
E	?	?	?	4	?

	A	B	C	D	E
A	0	4	5	5	7
B	3	0	1	4	6
C	2	6	0	3	5
D	3	7	1	0	2
E	1	5	5	4	0

Step 6: Using Node E as the Intermediate node

Distance[i][j] = min (Distance[i][j], Distance[i][E] + Distance[E][j])

	A	B	C	D	E
A	?	?	?	?	7
B	?	?	?	?	6
C	?	?	?	?	5
D	?	?	?	?	2
E	1	5	5	4	0

	A	B	C	D	E
A	0	4	5	5	7
B	3	0	1	4	6
C	2	6	0	3	5
D	3	7	1	0	2
E	1	5	5	4	0

Step 7: Return Distance[ ][ ] matrix as the result

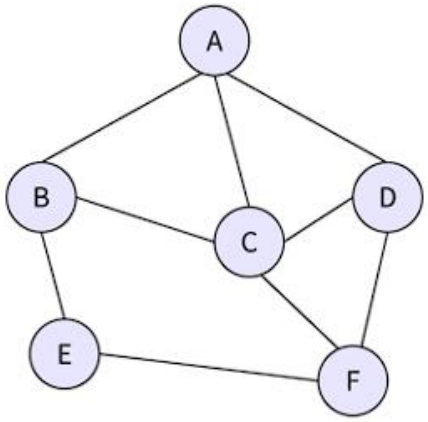
	A	B	C	D	E
A	0	4	5	5	7
B	3	0	1	4	6
C	2	6	0	3	5
D	3	7	1	0	2
E	1	5	5	4	0

3. Flooding:

Flooding is a **static routing technique**, based on the following principle:

"When a packet reaches the router, it is transferred to all the outgoing links, except only the link that it has reached the router through."

Flooding is used in routing protocols such as O.S.P.F. (Open Shortest Path First), peer-to-peer file transfers, systems such as Usenet, bridging, etc. Let us have a look at an example for a better understanding. Assume there is a network with **6 routers** connected through transmission lines, as shown in the figure ahead.



Following are the Events That Take Place in Flooding:

- Any packet incoming to A is sent to D, C, and B.
- B sends this packet to E and C.
- C sends this packet to F, D, and B.
- D sends this packet to F and C.
- E sends the packet to F.
- F sends the packet to E and C.

Types of Flooding:

Flooding in computer networking is usually of the following **three kinds**:

1. Uncontrolled Flooding: In uncontrolled flooding, every **node distributes the packets unconditionally** to all its neighbors. Broadcast storms become a catastrophe in the absence of conditional logic for the **prohibition of indefinite recirculation** of the same packet.

2. Controlled Flooding: Controlled flooding is **more reliable**, thanks to the two algorithms that it has:

I. **S.N.C.F. (Sequence Number Controlled Flooding):** As each node possesses **sequence numbers and memory of addresses**, it sticks its very own sequence number and addresses with the packet. If a packet arrives at a node that has the packet in memory already, the node immediately drops the packet.

II. **R.P.F. (Reverse Path Forwarding):** A node transfers a packet only in the **forward direction** to the next node. If the packet came from the next node, it is **returned to the sender**.

3. Selective Flooding: It is a version of flooding that only **sends packets to routers in the same direction**. Instead of transferring each incoming packet on every line, the routers transmit the packets on only those lines that are approximately going in the **right direction**.

Characteristics of Flooding:

Following are some features of flooding:

- Every possible route between the source and the destination for transmission is tried in flooding.
- There always exists a **minimum of one route** which is the shortest.
- Any node that is **connected**, whether **directly or indirectly**, is explored.
- Flooding does not require any information related to the network, such as the costs of various paths, load conditions, topology, etc. This is why it is **non-adaptive**.

Advantages of Flooding:

- Flooding always attempts to select the **shortest path**.
- Since any node connected **directly or indirectly** is explored, there is no probability of any node being missed out.
- Flooding is **very robust**. Even if several routers malfunction, the packets still find a path to their destinations.
- Flooding is quite easy to implement and set up, as a router can know only about its neighbors.

Disadvantages of Flooding:

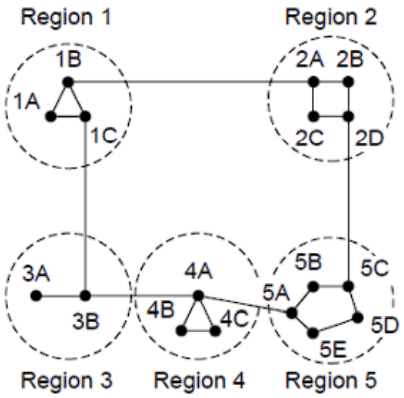
- **Repetitive and unauthorized packets** of data can jam a network. This could result in hampering other data packets.

- Flooding becomes **inefficient** in case only one destination requires the packet because flooding unconditionally transmits the data packet to all nodes.
- Flooding aids in generating an **infinite number of duplicate data packets** unless there exists some logic to enforce a limit upon the creation of packets.
- Flooding is expensive in terms of the bandwidth that it wastes. A message may have a single destination, yet it has to be sent to all the hosts.
- When a D.O.S. (Denial Of Service) attack or ping flood occurs, flooding may harm the reliability of the network.

4. Hierarchical Routing:

The routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

- Figure (a) gives a quantitative example of routing in a two-level hierarchy with five regions.
- The full routing table for router 1A has 17 entries, as shown in Fig. (b).

- When routing is done hierarchically, as in Fig. (c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B-2A line, but the rest of the remote traffic goes via the 1C-3B line.
- Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.

Example: If the same subnet of 720 routers is partitioned into 8 clusters, each containing 9 regions and each region containing 10 routers. Then what will be the total number of table entries in each router?

Solution:

10 local entries + 8 remote regions + 7 clusters = 25 entries.

5. Broadcast Routing:

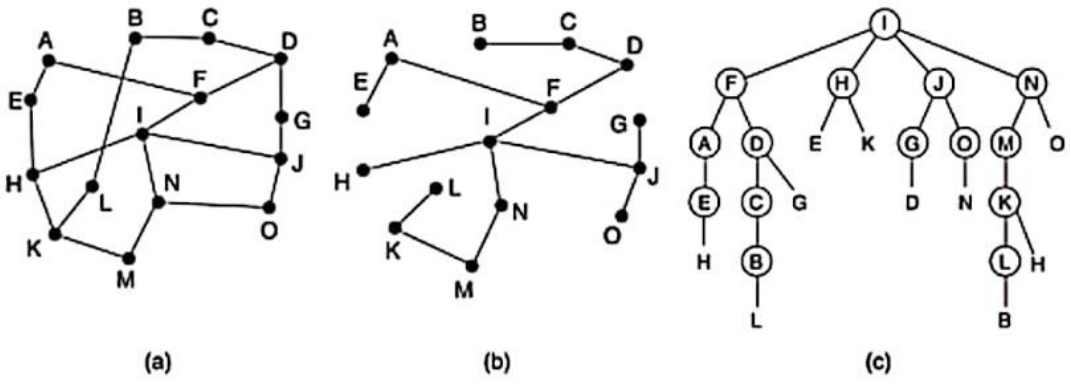
Sending a packet to all destinations simultaneously is called **broadcasting.**

It involves transmitting data, messages, or signals from one source to destinations within a network. Unlike routing (one-to-one communication) or multicast routing (one-to-many communication) broadcast routing ensures that information reaches all devices or nodes within the network.

1) The source simply sends a distinct packet to each destination. Not only is the method wasteful of bandwidth, but it also requires the source to have a complete list of all destinations.

2) **Flooding:**

The problem with flooding as a broadcast technique is that it generates too many packets and consumes too much bandwidth.



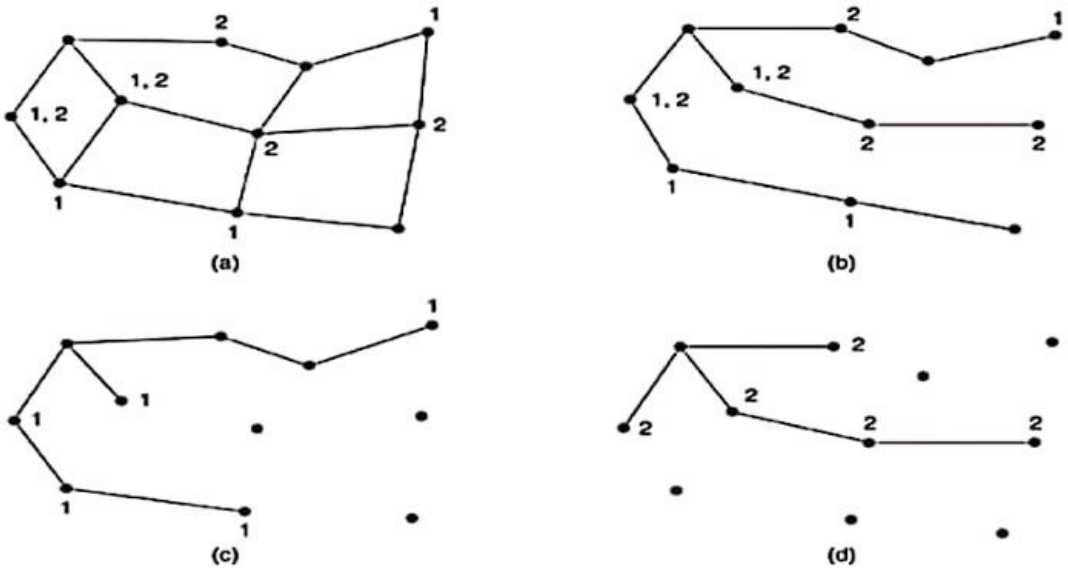
Reverse path forwarding. (a) A subnet. (b) A sink tree. (c) The tree built by reverse path forwarding.

Part (a) shows a subnet, part (b) shows a sink tree for router I of that subnet, and part (c) shows how the reverse path algorithm works.

When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast. If so, there is an excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router.

This being the case, the router forwards copies of it onto all lines except the one it arrived on. If, however, the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.

6. Multicast Routing:



- To do multicast routing, each router computes a spanning tree covering all other routers. For example, in Fig. (a) we have two groups, 1 and 2.

- Some routers are attached to hosts that belong to one or both of these groups, as indicated in the figure.

- A spanning tree for the leftmost router is shown in Fig. (b). When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.

- In our example, Fig. (c) shows the pruned spanning tree for group 1. Similarly, Fig. (d) shows the pruned spanning tree for group 2. Multicast packets are forwarded only along the appropriate spanning tree.

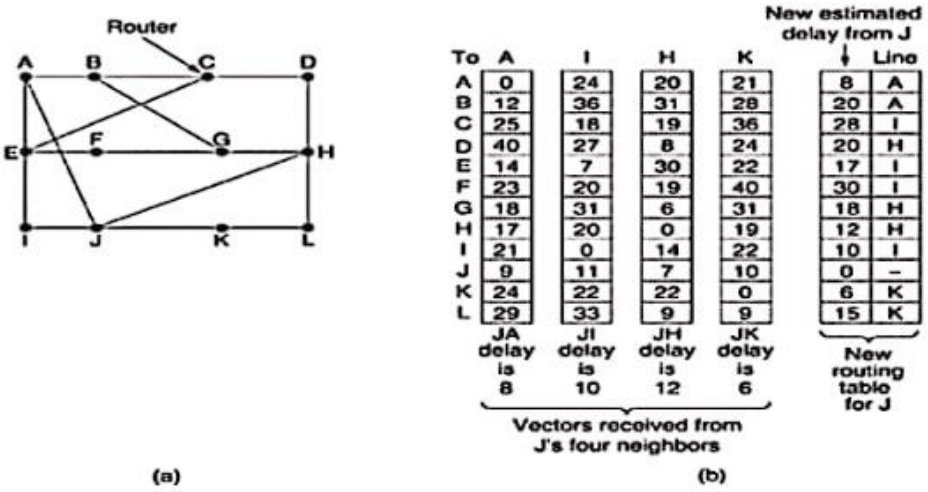
Distance Vector Routing:

Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there.

These tables are updated by exchanging information with the neighbors.

The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962).

It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP.



(a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.

Part (a) shows a subnet. The first four columns of part (b) show the delay vectors received from the neighbours of router J.

A claims to have a 12-msec delay to B, a 25-msec delay to C, a 40-msec delay to D, etc. Suppose that J has measured or estimated its delay to its neighbours, A, I, H, and K as 8, 10, 12, and 6 msec, respectively.

Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.

2. A link that is down is assigned an infinite cost.

Example:

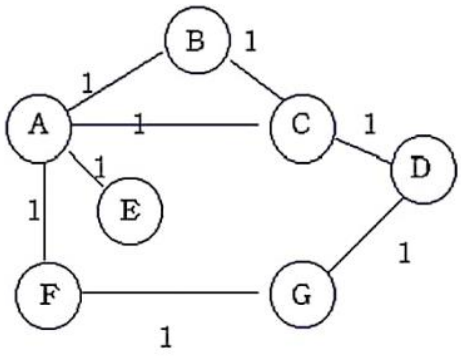


Table 1. Initial distances stored at each node(global view).

Information	Distance to Reach Node						
Stored at Node	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

Table 2. final distances stored at each node (global view).

Information	Distance to Reach Node						
Stored at Node	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

In practice, each node's forwarding table consists of a set of triples of the form: (Destination, Cost, NextHop).

For example, Table 3 shows the complete routing table maintained at node B for the network in figurel.

Table 3. Routing table maintained at node B.

Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

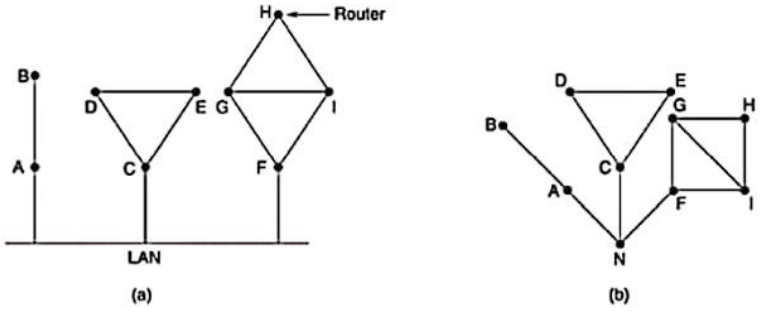
Link State Routing:

The idea behind link state routing is simple and can be stated as five parts. Each router must do the following:

1. Discover its neighbors and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router

Learning about the Neighbours:

When a router is booted, its first task is to learn who its neighbours are. It accomplishes this goal by sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is.



(a) Nine routers and a LAN. (b) A graph model of (a).

Measuring Line Cost:

- The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors. The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.
- By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.
- For even better results, the test can be conducted several times, and the average used. Of course, this method implicitly assumes the delays are symmetric, which may not always be the case.

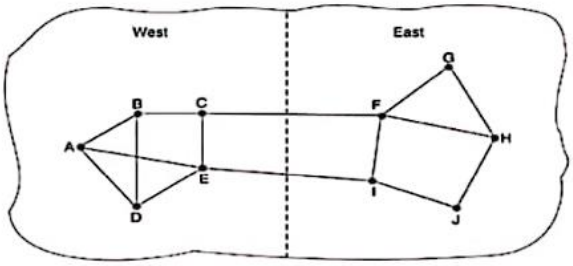
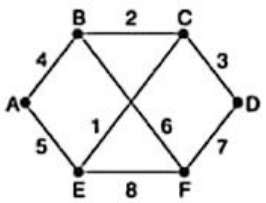


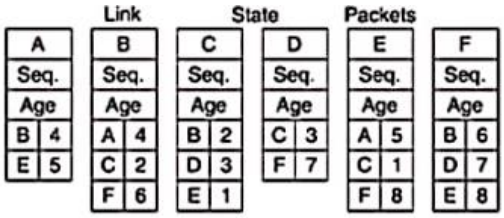
Figure: A subnet in which the East and West parts are connected by two lines.

- Unfortunately, there is also an argument against including the load in the delay calculation. Consider the subnet of Fig., which is divided into two parts, East and West, connected by two lines, CF and El.

Building Link State Packets:



(a)



(b)

(a) A subnet. (b) The link state packets for this subnet.

- Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data.
- The packet starts with the identity of the sender, followed by a sequence number and age (to be described later), and a list of neighbours.
- For each neighbour, the delay to that neighbour is given.
- An example subnet is given in Fig. (a) with delays shown as labels on the lines. The corresponding link state packets for all six routers are shown in Fig. (b).

Distributing the Link State Packets:

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

The packet buffer for router* B *in Fig. 5-13.

In above Fig., the link state packet from A arrives directly, so it must be sent to C and F and acknowledged to A, as indicated by the flag bits.

Similarly, the packet from F has to be forwarded to A and C and acknowledged to F.

Difference Between Distance Vector Routing and Link State Routing:

S.No.	Distance Vector Routing	Link State Routing
1.	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
2.	Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
3.	Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
4.	Traffic is less.	Traffic is more.
5.	Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
6.	Count of infinity problem.	No count of infinity problem.
7.	Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
8.	Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

Congestion Control:

Congestion control in computer networks refers to the set of techniques, mechanisms, and protocols designed to manage and regulate the flow of data traffic within a network to prevent congestion. It is a vital aspect of network management, aimed at ensuring the efficient and reliable transfer of data while avoiding the degradation of network performance due to overload.

When the demand for network resources exceeds its capacity, congestion occurs. Similar to traffic congestion on busy roads, network congestion leads to delays, increased latency, packet loss, and reduced throughput. This can severely impact the overall user experience, hinder critical applications, and result in a loss of productivity and revenue for businesses.

The primary goal of congestion control is to balance the usage of available network resources, preventing any single component from becoming overwhelmed. It achieves this by actively monitoring network conditions, detecting congestion indicators, and taking appropriate actions to alleviate congestion or prevent it from occurring in the first place.

Effects of Congestion Control:

Here are some of the key effects of congestion control:

- **Improved Network Stability:** Congestion control prevents network resources from becoming overwhelmed, which helps maintain network stability. By regulating the flow of data and ensuring that the network operates within its capacity limits, congestion control reduces the likelihood of network failures or crashes due to congestion-related issues.
- **Reduced Latency and Packet Loss:** Congestion can lead to increased latency, causing delays in data transmission. With congestion control mechanisms in place, the network can better manage data traffic, leading to reduced latency and minimizing packet loss. This results in faster data transfers and a more responsive network.
- **Enhanced Throughput:** By preventing congestion, congestion control allows for the optimal utilization of network resources. This leads to improved throughput, allowing more data to be transmitted in a given time, which is crucial for handling large data volumes and supporting high-bandwidth applications.
- **Fairness in Resource Allocation:** Congestion control algorithms, such as TCP, are designed to allocate network resources fairly among different flows or connections. This ensures that no single application or user dominates the available resources, promoting a balanced distribution of bandwidth.

- **Better User Experience:** Smooth data flow and reduced latency translate to an enhanced user experience. With congestion control in place, users can access online services, websites, and applications more reliably and without frustrating delays.
- **Mitigation of Network Congestion Collapse:** In the absence of congestion control, network congestion can snowball into a phenomenon known as "congestion collapse." This occurs when a sudden surge in data traffic overwhelms the network, leading to widespread congestion and rendering the network almost unusable. Effective congestion control helps prevent such catastrophic scenarios.

Congestion Control Algorithms:

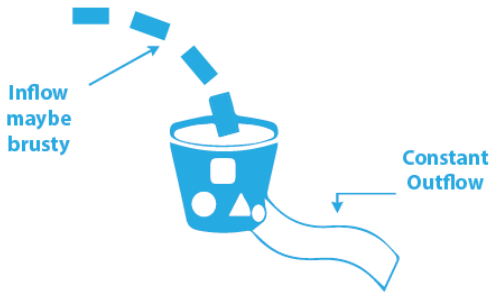
- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse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

1. Leaky Bucket Algorithm:

- The leaky bucket method finds applications for shaping or rate-limiting network traffic.
- For traffic shaping algorithms, a token bucket execution and a leaky bucket execution are typically utilized.
- With the help of this method, the network's transmission rate may be managed, and burst traffic can be turned into a constant stream.
- When compared to the leaky-bucket algorithm, the drawbacks include the ineffective utilization of available network resources.
- The bandwidth and other extensive network resources are not being utilized efficiently.

To further understand, let's look at an example.

Think of a bucket that has a tiny hole in the bottom. No matter how quickly water enters the bucket, the pace at which it exits remains constant. Water that is added after the bucket is full flows over the edges and is lost.



Similar to this, each network interface has a leaky bucket, and the leaky bucket method involves the following steps:

- Packets are dropped into the bucket when the host wants to send them.
- The network interface broadcasts packets at a consistent pace because the bucket leaks at a constant rate.
- The leaky bucket converts chaotic traffic into regular traffic.
- The bucket actually functions as a finite queue with a finite rate of output.

2. Token bucket Algorithm:

- The output architecture of the leaky bucket method is stiff at an average rate irrespective of the bursty traffic.
- When there are significant bursts, certain applications allow the output to accelerate. This needs a more adaptable algorithm, ideally one that never loses data. A token bucket approach is thus useful for rate-limiting or filtering network traffic.
- It is a control algorithm that suggests the best times to send traffic. Based on how many tokens are visible in the bucket, this ranking is generated.
- Tokens are in the bucket. Each token designates a packet of a specific size. To allow sharing of a packet, tokens in the bucket are erased.
- When tokens are displayed, a flow of transmit traffic also does so.
- If there is no token, no flow will send packets. As a result, a flow transfers traffic in good tokens in the bucket up to its peak burst rate.

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 the token bucket algorithm.

Steps of this algorithm can be described as follows:

- In regular intervals tokens are thrown into the bucket.
- The bucket has a maximum capacity.
- 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.

Let's understand with an example,

In figure (A) 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. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

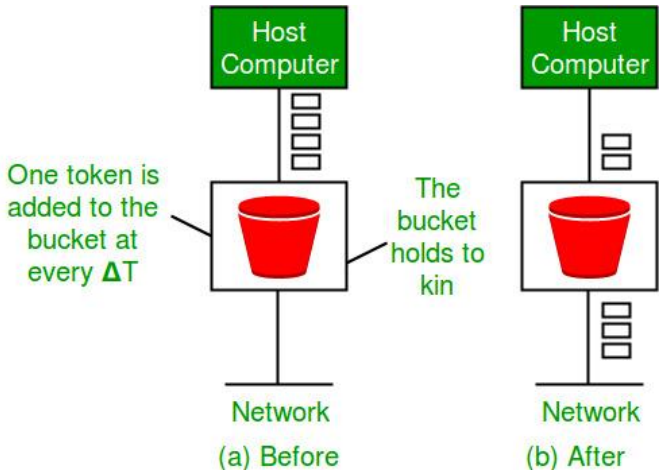
Ways in which token bucket is superior to leaky bucket:

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 + ? * s

where S – is time taken, M – Maximum output rate, ? – Token arrival rate, C – Capacity of the token bucket in byte

Let's understand with an example,



Quality of Service:

Quality of Service (QoS) is basically the ability to provide different priority to different applications, users, or data flows, or in order to guarantee a certain level of performance to the flow of data.

In other words, we can also define **Quality of Service** as something that the flow seeks to attain.

QoS is basically the overall performance of the computer network. Mainly the performance of the network is seen by the user of the Network.

Flow Characteristics:

Given below are four types of characteristics that are mainly attributed to the flow and these are as follows:

1. Reliability: It is one of the main characteristics that the flow needs. If there is a lack of reliability then it simply means losing any packet or losing an acknowledgement due to which retransmission is needed. Reliability becomes more important for electronic mail, file transfer, and for internet access.

2. Delay: Another characteristic of the flow is the delay in transmission between the source and destination. During audio conferencing, telephony, video conferencing, and remote conferencing there should be a minimum delay.

3. Jitter: It is basically the variation in the delay for packets that belongs to the same flow. Thus, Jitter is basically the variation in the packet delay. Higher the value of jitter means there is a large delay and the low jitter means the variation is small.

4. Bandwidth: The different applications need different bandwidth.

How to achieve Quality of Service?

Let's get into some details and say, your organization wants to achieve Quality of Service, which can be done by using some tools and techniques, like **jitter buffer** and **traffic shaping**.

Jitter buffer:

This is a **temporary storage buffer** which is used to store the incoming data packets, it is used in **packet-based networks** to ensure that the **continuity of the data streams** doesn't get disturbed, it does that by **smoothing out the packet arrival** times during periods of network congestion.

Traffic shaping:

This technique which is also known as **packet shaping** is a **congestion control or management technique** that helps to regulate network data transfer by delaying the flow of least important or least necessary data packets.

QoS is included in the service-level agreement when an organization signs it with its network service provider which guarantees the selected performance level.

Queuing and Scheduling:

When a router (switch) receives packets from different flows, it stores them in different buffers we call queues. We differentiate the traffic in queues by order of priority. Packets belonging to the same type of class form a singular queue. Based on the result of classification, each traffic receives a specific type of treatment.

There are three techniques for scheduling queues: First-In-First-Out (FIFO) queuing, priority queuing, and weighted fair queuing, where we weigh the queues using their priorities.

Three of them here-

- **FIFO Queuing** Packets wait in a buffer (queue) in first-in, first-out (FIFO) queuing until the node (router or switch) is prepared to process them. The queue will get full and new packets will be deleted if the average arrival rate exceeds the average processing rate. Anyone who has had to wait at a bus stop for a bus knows what a FIFO queue is like.
- **Priority Queuing** Packets are first given a priority class in priority queuing. Each type of priority has its own queue. The first packets processed are those in the queue with the highest priority. The final packets processed are those in the lowest priority queue. The system continues to serve a queue until it is empty, it should be noted.
- **Weighted Fair Queuing** The packets are still allowed to various queues and assigned to various classes in this method. The queues are, however, weighted according to their priority; a higher priority corresponds to a higher weight. The quantity of packets processed from each queue is determined by the associated weight, and the system processes packets in each queue in a round-robin method.

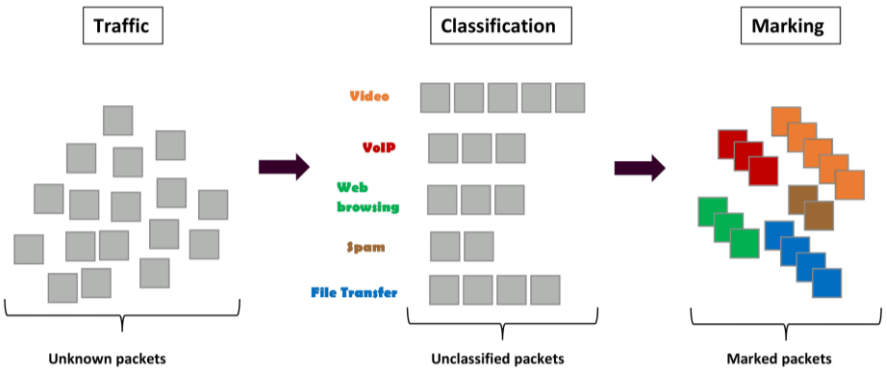
Classification and Marking:

Here, we split the network traffic into different classes. Grouping distinct packets having the same class (video, audio, web browsing, etc.) helps us know what types of data streams flow across the network and how to assign priorities.

Usually, **we distinguish traffic classes by their level of priority as sensitive traffic (such as voice over IP (VoIP) and video conferencing), best-effort traffic like emailing, and undesirable traffic such as spam.**

We label each packet with the appropriate class by changing a field in the packet header. This process is called marking, ensuring the network recognizes and prioritizes the sensitive ones.

Classification is sorting the packets for labeling. Both are implemented within a router or a switch:



There are 2 types of Quality-of-Service Solutions:

1. **Stateless Solution:** Here, the server is not required to keep or store the server information or session details to itself. The routers maintain no fine-grained state about traffic, one positive factor of this is, that it's **scalable and robust**. But also, it has weak services as there is **no guarantee about the kind of performance delay** in a particular application which we encounter. In the stateless solution, the server and client are **loosely coupled** and can act.
2. **Stateful Solution:** Here, the server is required to maintain the **current state and session information**, the **routers maintain per-flow state** as the flow is very important in providing the Quality-of-Service which is providing powerful services such as guaranteed services and high resource utilization, provides protection, and is much **less scalable and robust**. Here, the server and client are **tightly bounded**.

Quality of Service Parameters:

QoS can be measured quantitatively by using several parameters

- **Packet loss:** it happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.

- **Jitter:** occurs as the result of network congestion, timing drift, and route changes. And also, too much jitter can degrade the quality of audio communication.
- **Latency:** is the time delay, which is taken by a packet to travel from its source to its destination. For a great system, latency should be as low as possible, ideally, it should be close to zero.
- **Bandwidth:** is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time. QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.
- **Mean opinion score:** it is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

Implementing Quality of Service:

We can implement Quality of service through three of the following existing models:

1. **Best Effort**: if we are applying this model then, it means that we are prioritizing all the data packets equally. But since we all setting the priority order like this, then there is no guarantee that all the data packets will be delivered, but it will put up the best effort to deliver all of them. Point to remember is, that the best-effort model is applied when networks haven't configured with the QoS policies or incase their network infrastructure does not support QoS.
2. **Integrated Services**: or IntServ, this QoS model reserves the bandwidth along a specific path on the network. The applications ask the network's resource reservation for themselves and parallelly the network devices monitor the flow of packets to make sure network resources can accept packets. Point to remember: while implementing Integrated Services Model, the IntServ-capable routers and resource reservation protocol are necessary. This model has limited scalability and high consumption of the network resources.
3. **Differentiated Services**: in this QoS model, the network elements such as routers and switches are configured to serve multiple categories of traffic with different priority orders. A company can categorize the network traffic based on its requirements. Eg. Assigning higher priority to audio traffic etc.

Let us understand the difference between Integrated Services and Differentiated Services:

Integrated Services	Differentiated Services
This Architecture mainly specifies the elements to guarantee Quality of Service (QoS) on the network.	This Architecture mainly specifies a simple and scalable mechanism for classifying and managing the traffic of the network and also provides QoS on the modern IP networks.
These services mainly involve the prior reservation of the resources before sending in order to achieve Quality of Service.	These services mark the packets with the priority and then sends it to the network and there is no concept of prior reservation.
It is also known as IntServ.	It is also known as DiffSer.
These are not Scalable	These are Scalable.
These involve per flow Setup	These involve long term Setup
In this end to end service scope is available.	In this domain service scope is involved

Internetworking:

Internetworking, often called interconnecting networks, is the practice of connecting different computer networks or network segments to create a larger and more extensive network infrastructure. Various networking technologies, protocols, and devices, including routers and switches, are used to enable communication and data exchange between these distinct networks.

The term internetworking is made up of two words, inter and networking, which refers to a link between two or more separate nodes/segments. Internetworking aims to establish a seamless and cohesive network environment in which data can transfer efficiently and effectively across several interconnected networks, regardless of their underlying technologies or architectures.

There is a slight difference between network expansion and Internetworking. Using a switch or hub to link two local area networks constitutes a LAN extension, whereas employing a router to connect them exemplifies internetworking. Internetworking operates within Layer 3 (Network Layer) of the OSI-ISO model. The most popular example of internetworking is the Internet.

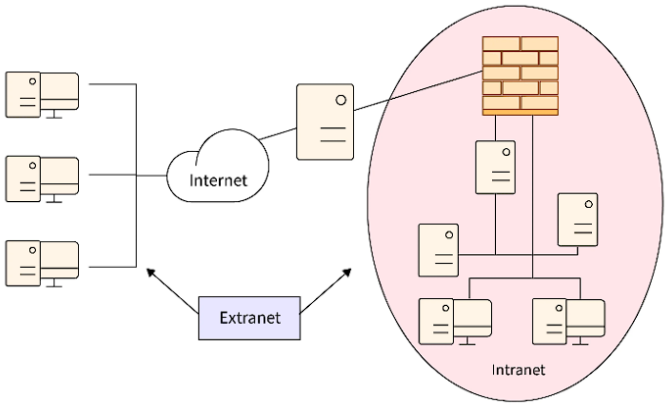
How does It Work?

Internetworking establishes connections between distinct computer networks, allowing them to communicate and share data effectively. Every individual network node or phase is built with a similar protocol or communication logic, such as **Transfer Control**

Protocol (TCP) or **Internet Protocol (IP)**, to enable communication. Internetworking occurs when one network communicates with another using constant communication processes. The goal of internetworking was to overcome the problem of sending a packet of data across several lines.

Types of Internetworking:

The three types of internetworking are as follows:



1. Extranet:

In computer networks, an extranet refers to a controlled and secure extension of an organization's internal network that allows authorized external parties, such as clients, partners, suppliers, or customers, to access certain resources, services, and information.

It is a network of internetwork that is restricted in scope to one organization or entity but also has restricted links to the networks of one or more other organizations or entities at times, but not always. It is the most basic level of Internetworking, usually imposed in an extremely private place. Although an extranet may be classed as a Man, WAN, or another type of network, it cannot include a single local area network and must include at least one reference to an external network.

2. Intranet:

An intranet is a private and internal network within a company that uses internet protocols and technology to allow employees or members to share information, resources, and services. It functions similarly to the internet but is limited to the members of the organization. Intranets are used for internal communication, document sharing, project collaboration, and access to internal tools and applications.

This type of computer network is a compilation of interconnected networks that leverage the Internet Protocol and employ IP-based tools such as web browsers and FTP applications. It operates under the jurisdiction of a single administrative entity. This entity restricts external access to the network, permitting entry exclusively to designated

users. Commonly, this network functions as the internal infrastructure of a corporation or another business entity. In larger instances, this network may incorporate its web server, enabling users to access and navigate through available information.

3. Internet:

The internet, short for **interconnected network**, is a global network of interconnected computers and computer networks that communicate with one another via standardized protocols. It is an immense network that allows people, organizations, and computers all over the world to share information, resources, and services.

It is a specific Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks primarily based on the Advanced Research Projects Agency Network (ARPANET) developed by **ARPA of the United States Department of Defence** and also home to the **World Wide Web (WWW)** and referred to as the 'Internet' to distinguish it from all other generic Internetworks. Participants on the internet, as well as their service providers, use IP addresses obtained from address registries that control assignments.

Internetwork Addressing:

Data Link Layer Addresses:

Data-link layer addresses serve as distinct identifiers for the physical network connections of network devices. These addresses, often referred to as hardware addresses or MAC addresses, are commonly utilized to uniquely identify devices within a network. They can be organized hierarchically or in a flat manner. Data-link addresses are typically pre-assigned to devices and remain constant for a specific device.

End systems typically possess a single data-link address due to their singular physical network connection. Conversely, routers and other internetworking components often feature multiple data-link addresses due to their numerous physical network associations.

MAC Addresses:

MAC addresses are essential elements of the data-link layer, defining network identities within **IEEE-assigned** MAC address-based local area networks (LANs). Each local area network interface has a unique MAC address that represents a single network unit. These addresses have twelve hexadecimal digits and a length of forty-eight bits. The first twelve digits are the Organisational Unique Identifier (OUI), which is frequently handled by the IEEE and identifies the manufacturer or vendor.

The last six hexadecimal digits reflect the interface serial number or another value specified by the manufacturer. These MAC addresses are automatically copied from read-only memory (ROM) to random-access memory (RAM) during interface card activation. They are also known as **burned-in addresses (BIAs)**.

Network Layer Addresses:

Network addresses can appear in both structured address spaces and the more common virtual or logical address spaces. The relationship between the network address and the device is flexible and conceptual in nature. It frequently relies on elements such as physical network features or arbitrary groups rather than exact physical properties. Each network-layer protocol that an end system supports requires a network-layer address.

Similarly, routers and other internetworking equipment necessitate a distinct network-layer address for each physical network connection within their support for each network-layer protocol.

Note: IP addresses in computer networks come in two main types: IPv4 and IPv6. IPv4, using 32-bit numbers like 192.168.1.1, faces scarcity issues. IPv6, with 128 bits in hexadecimal like 2001:0db8:85a3::8a2e:0370:7334, solves this problem.

Challenges to Internetworking:

Internetworking comes with several challenges due to its complexity and the diverse technologies and systems involved. Some of the challenges include:

- **Scalability**: As the number of devices and users on a network increases, the network must be able to handle growing traffic, data, and demands without incurring major performance degradation. It is a continuing struggle to design networks that can scale effectively.
- **Security**: As networks become more connected, the potential attack surface for malicious actors grows. Protecting networks from unauthorized access, data breaches, viruses, and other online threats is an essential concern in internetworking.
- **Reliability and Redundancy**: Networks need to be highly reliable, minimizing downtime and disruptions. Implementing redundancy mechanisms and failover systems to ensure continuous operation in the face of failures is complex but necessary.
- **Interoperability**: Different networks and devices frequently employ a variety of protocols, standards, and technologies. It can be difficult to ensure smooth communication and compatibility among these disparate elements. Protocols such as TCP/IP have helped bridge these gaps, although problems can still exist.

- **Network Management**: As networks grow in complexity, managing and monitoring them becomes increasingly challenging. Efficiently diagnosing and troubleshooting issues, optimizing performance, and ensuring proper resource allocation are ongoing tasks.
- **Resource Management**: It can be difficult to manage network resources properly to ensure optimal performance, especially in shared environments. This includes responsibilities such as bandwidth allotment and congestion control.

Advantages of Internetworking:

- **Global Connectivity**: Internetworking provides worldwide connectivity, allowing users and devices to communicate and exchange resources from all over the world.
- **Scalability**: Internetworking allows networks to scale to accommodate growing numbers of users and devices without needing to rebuild the entire infrastructure.
- **Resource Sharing**: Users can share resources such as files, printers, and databases across networks, increasing efficiency and collaboration.
- **Remote Access**: Internetworking facilitates remote access to corporate networks, enabling telecommuting and remote management.
- **Redundancy and Failover**: Redundant network connections and failover mechanisms improve network reliability, minimizing downtime and ensuring continuous operation.

Disadvantages of Internetworking:

- **Security Risks**: Internetworking exposes networks to additional security concerns such as unauthorized access, data breaches, and cyberattacks.
- **Network Congestion**: Increased connectivity can cause network congestion and poor performance, particularly during high usage times.
- **Privacy Concerns**: Internetworking raises concerns about user privacy and data protection, particularly when sensitive information is transmitted across networks.
- **Dependency on Infrastructure**: Organizations that rely on interconnected networks are vulnerable to outages or interruptions in the internet infrastructure.
- **Complexity**: Connecting multiple networks using different technologies and protocols creates complexity in terms of configuration, management, and troubleshooting.

Fragmentation:

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held in a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from the transport layer into fragments so that data flow is not disrupted.

Important Points About Fragmentation:

- Since there are 16 bits for total length in IP header so, the maximum size of IP datagram = $2^{16} - 1 = 65,535$ bytes.
- It is done by the network layer at the destination side and is usually done at routers.
- Source side does not require fragmentation due to wise (good) segmentation by transport layer i.e. instead of doing segmentation at the transport layer and fragmentation at the network layer, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without the need of fragmentation.
- Receiver identifies the frame with the **identification (16 bits)** field in the IP header. Each fragment of a frame has the same identification number.
- Receiver identifies the sequence of frames using the **fragment offset (13 bits)** field in the IP header
- Overhead at the network layer is present due to the extra header introduced due to fragmentation.

Need of Fragmentation at Network Layer:

Fragmentation at the Network Layer is a process of dividing a large data packet into smaller pieces, known as fragments, to improve the efficiency of data transmission over a network. The need for fragmentation at the network layer arises from several factors:

1. Maximum Transmission Unit (MTU): Different networks have different Maximum Transmission Unit (MTU) sizes, which determine the maximum size of a data packet that can be transmitted over that network. If the size of a data packet exceeds the MTU, it needs to be fragmented into smaller fragments that can be transmitted over the network.

2. Network Performance: Large data packets can consume a significant amount of network resources and can cause congestion in the network. Fragmentation helps to reduce the impact of large data packets on network performance by breaking them down into smaller fragments that can be transmitted more efficiently.

3. Bandwidth Utilization: Large data packets may consume a significant amount of network bandwidth, causing other network traffic to be slowed down. Fragmentation helps to reduce the impact of large data packets on network bandwidth utilization by breaking them down into smaller fragments that can be transmitted more efficiently.

Fragmentation at the network layer is necessary in order to ensure efficient and reliable transmission of data over communication networks.

1.Large Packet Size: In some cases, the size of the packet to be transmitted may be too large for the underlying communication network to handle. Fragmentation at the network layer allows the large packet to be divided into smaller fragments that can be transmitted over the network.

2.Path MTU: The Maximum Transmission Unit (MTU) of a network defines the largest packet size that can be transmitted over the network. Fragmentation at the network layer allows the packet to be divided into smaller fragments that can be transmitted over networks with different MTU values.

3.Reliable Transmission: Fragmentation at the network layer increases the reliability of data transmission, as smaller fragments are less likely to be lost or corrupted during transmission.

Process of Fragmentation:

RFC 791 specifies IP packet fragmentation, transmission, and reassembly mechanism.

RFC 815 specifies a streamlined reassembly algorithm. The Identification field in the IP header, along with the foreign and local internet addresses and the protocol ID, and the Fragment offset field in the IP header, coupled with the Don't Fragment and More Fragments flags, are used for fragmentation and reassembly of IP packets.

If a receiving host receives a fragmented IP packet, it must put the packet back together and send it to the higher protocol layer. Reassembling is supposed to occur in the receiving host, but in reality, it might be carried out by an intermediate router. For instance, *network address translation (NAT)* can need to reassemble fragments to translate data streams.

Fields in IP header for fragmentation –

- **Identification (16 bits) –** use to identify fragments of the same frame.
- **Fragment offset (13 bits) –** use to identify the sequence of fragments in the frame. It generally indicates a number of data bytes preceding or ahead of the fragment. Maximum fragment offset possible = (65535 – 20) = 65515 {where 65535 is the

maximum size of datagram and 20 is the minimum size of IP header} So, we need ceil($\log_2 65515$) = 16 bits for a fragment offset but the fragment offset field has only 13 bits. So, to represent efficiently we need to scale down the fragment offset field by $2^{16}/2^{13} = 8$ which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset ∈ N.

- **More fragments (MF = 1 bit) –** tells if more fragments are ahead of this fragment i.e. if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.
- **Don't fragment (DF = 1 bit) –** if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

Reassembly of Fragments:

It takes place only at the destination and not at routers since packets take an independent path (datagram packet switching), so all may not meet at a router and hence a need of fragmentation may arise again. The fragments may arrive out of order also.

MF	Fragment Offset	
1	0	→ 1st packet
1	!=0	→ Intermediate packet
0	!=0	→ Last packet
0	0	→ Invalid

Algorithm –

1. Destination should identify that datagram is fragmented from MF, Fragment offset field.
2. Destination should identify all fragments belonging to same datagram from Identification field.
3. Identify the 1st fragment (offset = 0).
4. Identify subsequent fragments using header length, fragment offset.
5. Repeat until MF = 0.

Efficiency –

Efficiency (e) = useful/total = (Data without header)/(Data with header)

Throughput = e * B { where B is bottleneck bandwidth }

Example – An IP router with a Maximum Transmission Unit (MTU) of 200 bytes has received an IP packet of size 520 bytes with an IP header of length 20 bytes. The values of the relevant fields in the IP header.

Explanation – Since MTU is 200 bytes and 20 bytes is header size so, the maximum length of data = 180 bytes but it can't be represented in fragment offset since it is not divisible by 8 so, the maximum length of data feasible = 176 bytes.

Number of fragments = (520/200) = 3.

Header length = 5 (since scaling factor is 4 therefore, 20/4 = 5)

Efficiency, e = (Data without header)/(Data with header) = 500/560 = 89.2 %

	20 | 176	20 | 176	20 | 148
Fragment Offset	0	22	44
MF	1	1	0
Header length	5	5	5
Total length	196	196	168

Advantages of Fragmentation:

- It is used for network resources by allowing large data packets to be transmitted over a network.
- These have improved network reliability by reducing the likelihood of packet loss or corruption during transmission.
- They are compatible with different network technologies and protocols.
- The flexibility in accommodating varying network conditions and transmission requirements.

Disadvantages of Fragmentation:

- Increased overhead due to the additional packet headers needed for reassembly.
- Longer transmission times due to the need for reassembly at the destination.
- Increased likelihood of network congestion due to the higher number of packets generated.
- Greater susceptibility to security threats such as packet fragmentation attacks.

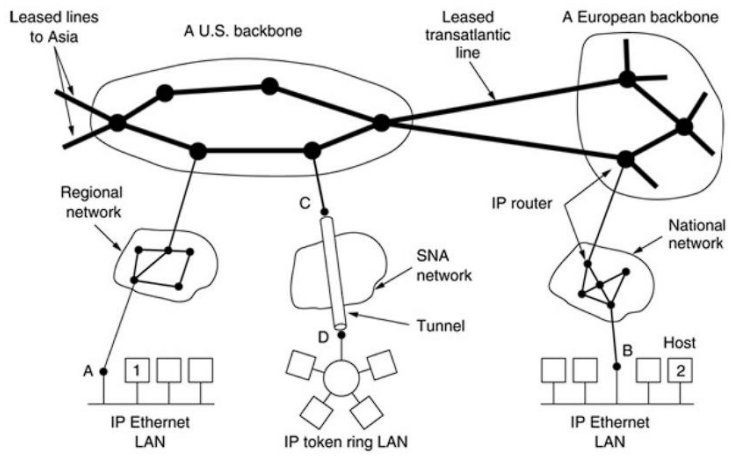
The Network Layer in the Internet:

At the network layer, the Internet can be viewed as a collection of subnetworks or autonomous systems that are connected together.

The glue that holds the Internet together is the network layer protocol, IP (Internet Protocol).

Communication in the Internet works as follows:

- The transport layer takes data streams and breaks them up into datagrams. In theory, datagrams can be up to 64 Kbytes each, but in practice they are usually around 1500 bytes.
- Each datagram is transmitted through the Internet, possibly being fragmented into smaller units as it goes.
- When all the pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram. This datagram is then handed to the transport layer, which inserts it into the receiving process input stream.



Collection of Subnetworks

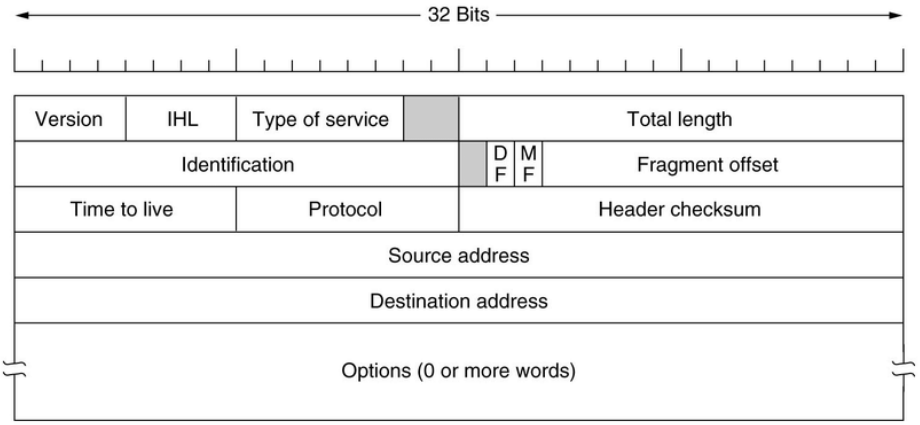
The Internet is an interconnected collection of many networks.

Design Principles for Internet:

1. Make sure it works.
2. Keep it simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. Think about scalability.
10. Consider performance and cost.

The IP Protocol:

- Communication in the Internet
- The transport layer takes data streams and breaks them up into datagrams.
- The datagrams can be up to 64 Kbytes each, but in practice they are usually not more than 1500 bytes (so they fit in one Ethernet frame).
- Each datagram is transmitted through the Internet, possibly being fragmented into smaller units as it goes.
- When all the pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.
- This datagram is then handed to the transport layer, which inserts it into the receiving process' input stream.



The IP Datagram

The IP protocol, pivotal in Internet communication, delineates the structure of IP datagrams, comprising a fixed 20-byte header and a variable-length optional part.

- **Version Field**: This field identifies the IP protocol version, facilitating transitions between versions as the Internet evolves over time.
- **IHL Field**: The Internet Header Length field specifies the length of the header in 32-bit words, allowing for flexibility in accommodating optional fields and extensions.
- **Type of Service Field**: Offering a spectrum of service types, this field allows hosts to express preferences based on priorities such as reliability and speed. However, modern routers often overlook these preferences.

• The Precedence field - priority, from 0 (normal) to 7 (network control packet)

• The three flag bits - allowed the host to specify what it cared most about from the set {Delay, Throughput, Reliability}

- **Total Length Field**: This field indicates the total length of the datagram, encompassing both the header and the data payload. The maximum length is currently set at 65,535 bytes.
- **Identification Field**: Used for reassembling fragments, this field aids in identifying which fragments belong to the same original datagram.
- **DF and MF Flags**: These flags control fragmentation behavior, with the DF (Don't Fragment) flag instructing routers not to further fragment the datagram, and the MF (More Fragments) flag indicating whether more fragments are expected.
- **Fragment Offset Field**: Indicates the position of each fragment within the original datagram, facilitating reassembly at the destination.
- **Time to Live Field (TTL)**: Serving as a hop counter, the TTL field limits the lifespan of a packet to prevent it from circulating endlessly in the network. When the TTL reaches zero, the packet is discarded, and an error message is sent back to the source.
- **Protocol Field**: This field specifies the transport protocol to which the datagram should be delivered, such as TCP, UDP, or others. It plays a crucial role in determining how the data should be handled at the transport layer.
- **Header Checksum**: Used to verify the integrity of the header, the checksum algorithm ensures that the header has not been corrupted during transmission.
- **Source and Destination Addresses**: These fields identify the network and host numbers of the sender and receiver, respectively, enabling routing and delivery of the datagram to the intended destination.
- **Options Field**: Designed for experimental features and extensibility, the options field provides flexibility for including additional information, such as security specifications, source routing instructions, and timestamps. However, many of these options are rarely utilized in practice due to their limited practical relevance in modern networking scenarios.

Some of the IP Option:

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

IP Addressing:

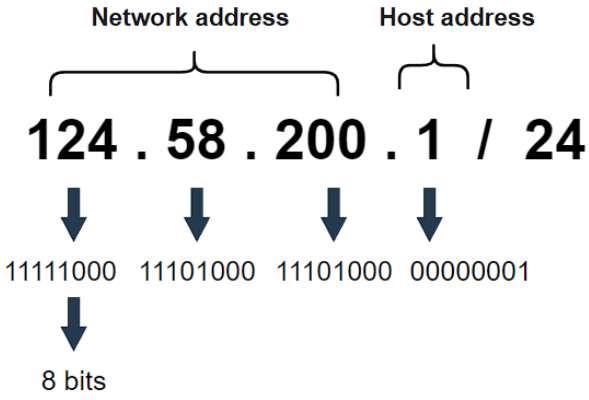
An Internet Protocol **(IP)** address is a unique identifier that assists in the recognition of different devices present over the network. Through **IP addressing**, we can send and receive data packets across the internet without trouble-free.

IP Format:

An IP address is a 32-bit numerical address separated by periods (.)(.) represented in dotted decimal notation. It is expressed in a set of four pairs, where each set ranges from 00 to 255255. Slash notation (/)(/) identifies the number of network bits reserved for the allocated IP address.

The Parts of an IP address:

The IP address has two parts: the **network address** and the **host address**. The network address is essential for the recognition of the network. In the host address part, we always reserve the first address for the network address, and the last address for the **broadcast address**. The broadcast address transmits data to all the hosts present in the network at once.



The format of an IP address

Types of IP Address:

There are mainly four types of IP addresses:

- Public,
- Private,
- Static
- Dynamic.

Among them, public and private addresses are based on their location of the network private, which should be used inside a network while the public IP is used outside of a network.

Let us see all these types of IP address in detail.

1. **Public IP Addresses:** A public IP address is an address where one primary address is associated with your whole network. In this type of IP address, each of the connected devices has the same IP address.

   This type of public IP address is provided to your router by your ISP.

2. **Private IP Addresses:** A private IP address is a unique IP number assigned to every device that connects to your home internet network, which includes devices like computers, tablets, smartphones, which is used in your household.

   It also likely includes all types of Bluetooth devices you use, like printers or printers, smart devices like TV, etc. With a rising industry of internet of things (IoT) products, the number of private IP addresses you are likely to have in your own home is growing.

3. **Dynamic IP address:** Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web. Dynamic IPs can trace their origin to a collection of IP addresses that are shared across many computers.

   Dynamic IP addresses are another important type of internet protocol addresses. It is active for a specific amount of time; after that, it will expire.

4. **Static IP Addresses:** A static IP address is an IP address that cannot be changed. In contrast, a dynamic IP address will be assigned by a Dynamic Host Configuration Protocol (DHCP) server, which is subject to change. Static IP address never changes, but it can be altered as part of routine network administration.

   Static IP addresses are consistent, which is assigned once, that stays the same over the years. This type of IP also helps you procure a lot of information about a device.

Types of Website IP Addresses:

Two types of website IP Addresses are -

1) Share IP Address 2) Dedicated IP Address

1. Shared IP Addresses: Shared IP address is used by small business websites that do not yet get many visitors or have many files or pages on their site. The IP address is not unique and it is shared with other websites.

2. Dedicated IP Addresses: Dedicated IP address is assigned uniquely to each website. Dedicated IP addresses helps you avoid any potential backlists because of bad behavior from others on your server. The dedicated IP address also gives you the option of pulling up your website using the IP address alone, instead of your domain name. It also helps you to access your website when you are waiting on a domain transfer.

Version of IP Address:

Two types of IP addresses are 1) IPV4 and 2) IPV6.

IPV4:

IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is the most widely used IP version. It is used to identify devices on a network using an addressing system.

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.

IPV6:

It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite is now called IPv6.

This new IP address version is being deployed to fulfill 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.

IP Address Classification Based on Operational Characteristics:

Unicast Addressing:

Unicast addressing is the most common concept of an IP address in the Unicast addressing method. It is available in both IPv4 and IPv6.

This IP address method refers to a single sender/receiver. It can be used for both sending and receiving the data.

In most cases, a Unicast address is associated with a single device or host, but a device or host that may have more than one unicast address.

Broadcast Addressing:

Broadcasting addressing is another addressing method available in IPv4. It allows you to manage data to all destinations on a network with a single transmission operation.

The IP address 255.255.255.255 is mostly used for network broadcast. Moreover, limited directed-broadcast uses the all-ones host address with the network prefix.

IPv6 does not provide any implementation and any broadcast addressing. It replaces it with multicast to the specially defined all-nodes of the multicast address.

Multicast IP Addresses:

Multicast IP addresses are used mainly for one-to-many communication. Multicast messages are mostly sent to the IP multicast group address.

In this, routers forward copies of the packet out to every interface with hosts subscribed to that specific group address. Only the hosts that require receiving the message will process the packets. All other hosts on that LAN will discard them.

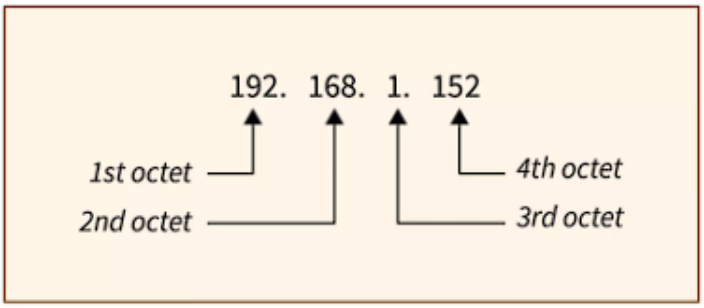
Anycast Addressing:

In anycast addressing the data, the stream is not transmitted to all receivers. However, just the one that the router decides is closest to the network.

This IP addressing comes as a built-in feature of IPv6. In IPv4, it is implemented by using the Border Gateway Protocol by using the shortest-path metric. This method is widely used for global load balancing and is also used in distributed DNS systems.

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.



Let us see the different notations of an IPv4 address:

Dotted Decimal	75.	45.	34.	78.
Binary	01001011	00101101	00100010	01001110
Hexadecimal	4B	2D	22	4E

Why Do We Use IPv4 Addressing?

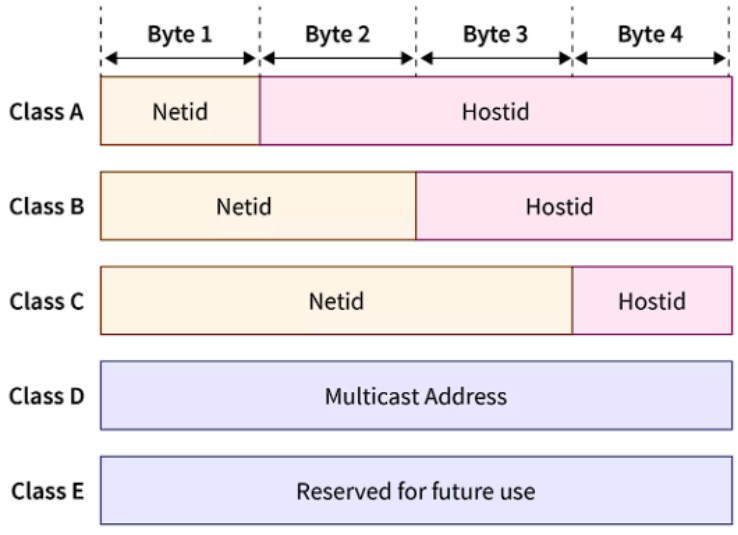
As discussed above, we need a unique address to identify the sender and the receiver so that the data can be transmitted after establishing the connection between the sender and the recipient. If our device wants to access other services on the internet, it needs a unique address i.e., the IP address.

The IPv4 address works on the network layer which is responsible for the transmission of data in the form of packets. It is a connectionless protocol. IPv4 uses a 32-bit address space which provides 4,294,967,296 (2^{32}) unique addresses, but large blocks are reserved for particular networking purposes.

Parts of IPv4:

As discussed at the start of the article, there are 2 parts of the IPv4 address- the network part and the host part. The network part is also known as the net id whereas the host part is also known as the host id.

Before we discuss them in-depth, let us first discuss the classes of IPv4 addresses. There are 5 types of classful addressing namely- **Class A**, **Class B**, **Class C**, **Class D**, and **Class E**. They are classified based on address space which is divided into a fixed number of blocks and has a fixed number of hosts.



Here, each class has a fixed number of hostid and netid. Now let us comprehend what the network part and host part means.

Network part: The network part is also known as **net id** which is used to classify the network to which the host is connected.

Host part: The host part is also known as the **host id** which is the part of the IP address which is used to uniquely identify the host on a network.

Characteristics of IPv4 Address:

- IPv4 addresses are 32-bit long.
- They are either represented in **binary**, **dotted-decimal**, or **hexadecimal** notation. The most common form to represent IPv4 addresses is the dotted decimal notation.
- IPv4 addresses are classified into classful addressing where the address space is divided into five classes- **Class A**, **Class B**, **Class C**, **Class D**, and **Class E**.
- IPv4 addresses are unique, so two devices on a network can never have the same IP address.
- IPv4 address consists of two parts - the network part and the host part.
- The IPv4 packet header consists of 20 bytes of data and the number of the header field is 12.
- IPv4 is a connectionless protocol.
- IPv4 has 3 modes of addressing- unicast, broadcast, and multicast.
- IPv4 can be assigned manually or by a protocol known as **DHCP** (Dynamic Host Configuration Protocol).
- IPv4 can be unreliable while transmitting packets.

Different Types of Addressing Modes in IPV4:

Addressing mode refers to the mechanism of hosting an address on a given network. There are three different types of addressing modes supported by IPv4.

Unicast addressing mode: As the name suggests, the data is sent to only a single host(uni=one). There is one source and one receiver. The relationship between the source and the destination network is one-to-one. The destination address field consists of a 32-bit IP address that belongs to the destination host. It is the most common mode of addressing.

Broadcast addressing mode: In broadcast addressing mode, the data is sent to all the devices in the network, i.e., multiple hosts. The destination address field of the packet consists of the IP address called the Special Broadcast address which is represented by 255.255.255.255255.255.255.255. The client then sends the packet which is received by all other servers on the network.

Multicast addressing mode: In multicasting addressing mode, there is one source and a group of destinations. The data, i.e., the packets are neither sent to one host nor multiple hosts but are instead sent to a group of hosts. The relationship between the source and the destination is one too many. The destination address consists of a special address starting with 224.*x*.*x*.*x*224.*x*.*x*.*x*.

Advantages of IPv4 Addressing:

- IPv4 is a connectionless protocol.
- The IPv4 routing can be handled easily by all the systems.
- Across a large network, IPv4 can connect various devices and along with connection, the verification can also be done. This is done without the use of **NAT** (Network Address Translation).
- The process of routing is carried out smoothly because the addresses are combined more effectively.
- Privacy and security are maintained in IPv4 as the data is encrypted in the packets.
- The encoding in IPv4 is flawless.

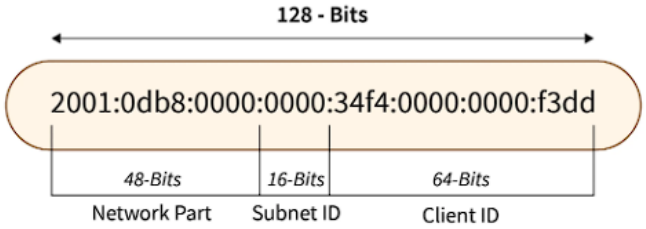
Disadvantages of IPv4 Addressing:

- IPv4 can be assigned manually or by a protocol known as DHCP and if it is done through DHCP, it needs a lot of management for its infrastructure.
- Since IPv4 was established way back, its implementation did not provide security against threats introduced today. **Internet Protocol Security** (IPSec) enables network security to IPv4 by specifying the use of the internet. However, the problem arises when IPSec is not built-in and its implementation is optional.
- Most of the IP addresses are reserved in the United States.
- To overcome the drawbacks of IPv4, IPv6 was introduced.

IPv6:

The new generation IP address, or IPv6, was created primarily to get over IPv4's limits and exhaustion. The 128-bit IPv6 protocol is made up of eight numbered strings with four (alphanumeric) characters each, separated by a colon. This provides us with an astounding number of unique IP addresses,

340,282,366,920,938,463,463,374,607,431,768,211,456 to be precise. Additionally, it guarantees that we won't soon run out of distinctive IP addresses to give to new gadgets.



Why Do We Need IPv6 Addressing?

1. **Address Exhaustion:** With the depletion of IPv4 addresses, IPv6 provides an extensive address space, accommodating the growing number of devices connected to the internet. This scalability ensures that every device, including those in the Internet of Things (IoT), can have a unique IP address.
2. **Security:** IPv6 incorporates built-in security features like IPsec, enhancing the overall security of internet communications. These features provide authentication, integrity, and confidentiality for data transmitted over IPv6 networks, addressing security concerns inherent in IPv4.
3. **Scalability:** IPv6's large address space allows for the seamless expansion of the internet and supports the deployment of new services and technologies. This scalability ensures that the internet can continue to grow and evolve to meet the demands of users and applications.
4. **Connectivity:** IPv6 enables improved connectivity by simplifying network configuration and management. It eliminates the need for techniques like Network Address Translation (NAT) used in IPv4, which can hinder end-to-end connectivity. IPv6's streamlined addressing and routing facilitate direct communication between devices, enhancing overall network connectivity.

Types of IPv6 Addresses:

There are three addressing methods available in IPv6 representation:

1. **Unicast Address** – A single network interface is detected by a unicast address. A unicast address directs a packet to the interface that the address designates.

2. **Multicast Address** – A group of hosts referred to as a multicast address purchases a multicast destination address. These hosts don't have to be close by geographically. All interfaces belonging to that multicast address will receive any packet transmitted to this multicast address.
3. **Anycast Address** – A collection of interfaces has been assigned an Anycast Address. Whenever a packet is sent to an anycast address, only one member interface will receive it.

Note:

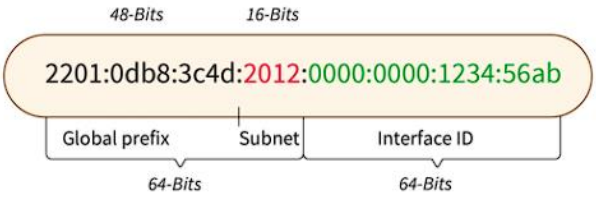
- The point of connection between a computer and a private or public network is known as a **network interface**. A network interface does not necessarily take the form of a physical **network interface card (NIC)**. The network interface can be replaced by software instead. For instance, **the loopback interface (127.0.0.1 for IPv4 and::1 for IPv6)** is a piece of software that simulates a network interface rather than a physical device.
- An address assigned to a collection of interfaces, often distributed among various routers, is known as an **anycast address**. When a packet is sent to an anycast address, it is sent to the nearest interface that also has that anycast address; the routing protocol decides which interface qualifies as "closest" in this case.

Format of the IPv6 Address:

128 bits make up an IPv6 address. In hexadecimal, IPv6 addresses are shown. Each 16-bit block of the 128-bit address is translated into a 4-digit hexadecimal integer, and colons are used to separate each block of 16 bits. The format of an IPv6 address is as follows:
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX, where each x represents 4 bits in hexadecimal notation.
From 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, IPv6 addresses fall inside this range.

A network component and a node component make up an IPv6 address. The first 64 bits of the address, known as the network component, are used for routing. The node component, which is the later 64 bits, is used to specify the interface's address.

A block of 48 bits and a block of 16 bits can be created from the network node. **Global network addresses** are stored in the upper 48 bits of the section. On an internal network, subnets are created using the lower 16-bit section, which is managed by network administrators.



Advantages of IPv6 Address:

- **Efficient Routing –** With IPv6, routing becomes more streamlined and hierarchical while also shrinking the size of routing tables. In IPv6 networks, the source device manages fragmentation using a protocol for the detection of the path's maximum transmission unit rather than a router.
- **Efficient Packet Processing –** The checksum does not need to be regenerated at each router hop because IPv6 does not include an IP-level checksum as IPv4 does.
- **Directed Data Flows –** Multicast is supported by IPv6 as opposed to broadcast. Network bandwidth can be conserved by using multicast to simultaneously send packet flows that use a lot of bandwidth to several destinations.
- **Security –** IPv6 is built using IPSec security, which offers data integrity, confidentiality, and authentication.

Disadvantages of IPv6 Address:

- The network infrastructure becomes overworked when routing table entries are needed for such a large number of networks.
- Older devices that do not support IPv6 must be manually set up using the Daul stack approach, adding extra effort for the network administrator.
- The globe is slow to switch to IPV6 and IPV4 is still widely used.

Difference Between IPv6 and IPv4:

IPv6	IPv4
IPv6 has a 128-bit address length	IPv4 has a 32-bit address length
It supports Auto and renumbering address configuration	It Supports Manual and DHCP address configuration
The address space of IPv6 is quite large it can produce 3.4×1038 address space	It can generate 4.29×109 address space

Address Representation of IPv6 is in hexadecimal	Address representation of IPv4 is in decimal
In IPv6 checksum field is not available	In IPv4 checksum field is available
IPv6 has a header of 40 bytes fixed	IPv4 has a header of 20-60 bytes.
IPv6 does not support VLSM.	IPv4 supports VLSM (Variable Length subnet mask).

Classless Inter-Domain Routing (CIDR):

Classless Inter-Domain Routing (CIDR) is a method used to combine numerous IP address ranges into one route or network. Also known as supernetting, it can reduce routing table size and make more IP addresses available within enterprise networks.

Every server, endpoint, and other machine that can connect to the internet has an IP address. This unique number can be used to track the device across the internet. Devices also use IP addresses to locate and communicate with each other.

CIDR is used by enterprises to allocate IP addresses efficiently and flexibly within their networks. Simply put, CIDR is a method used for IP address allocation to enhance the efficiency of data routing on the internet.

How Does CIDR Work?

Before we dive deeper into how CIDR works, we should understand IP address formats. An IP address has two parts:

- **Network address**, which is a series of numbers that defines the unique identifier of the network.
- **Host address**, which is a series of numerical digits that defines the identifier for the host or individual device within the network.

Before the turn of the millennium, IP address allocation would take place using the classful addressing system. The total length of the address was predefined, as was the number of bits allocated to the host and network segments.

What are classful addresses?

An IPv4 address is composed of 32 bits. Each string of numbers separated by the ‘full stop’ lies between 0 and 255 in numerical form and consists of 8 bits. Under the classful address system, enterprises had the option to purchase from among three classes of IPv4 addresses.

- **Class A addresses** with 8 network prefix bits (think 44.0.0.1 with 44 as the network address and 0.0.1 as the host address).
- **Class B addresses** with 16 network prefix bits (think 128.16.0.2 with 128.16 as the network address and 0.2 as the host address).
- **Class C addresses** with 24 network prefix bits (think 192.168.1.100 with 192.168.1 as the network address and 100 as the host address).

What are classless addresses?

Classless addresses, also known as CIDR, leverage variable length subnet masking (VLSM) to modify the ratio of network and host address bits in internet protocol addresses. Think of a subnet mask as an address that segregates an IP address into network bits (to identify the network) and host bits (to identify the host device operating on that network).

A VLSM sequence enables network admins to convert an IP address space into subnets of differing sizes. Each subnet can feature a flexible host count and a specific number of IP addresses. A CIDR IP address adds a suffix value that states the number of network address prefix bits to a normal IP address. For instance, 192.0.2.0/24 is an IPv4 CIDR address in which 192.0.2 (the first 24 bits) is the network address.

Limitations of Classful Addressing:

Classful IP addressing has two key limitations that CIDR addresses. Before CIDR, these classful address limitations gave rise to inefficiencies.

1. Low flexibility in IP addressing:

The classful addressing system allowed for each class to support a specific number of devices:

- Class A addresses were capable of supporting **16,777,214 hosts**.
- Class B addresses could support **65,534 hosts**.
- Class C addresses supported **254 hosts**.

This arrangement showed inefficiencies during the allocation of IP addresses and gave rise to the wastage of IP address space. For instance, an enterprise with 275 online devices could not opt for Class C IP addressing since this class only allowed up to 254 devices. Therefore, the enterprise would have had to opt for Class B IP addressing with 65,534 unique host addresses. However, with only 275 devices being connected, 65,259 IP address spaces would have been left unused.

2. Constraints in network design:

Classful IP addresses also limited the ability of the user to combine networks as needed. For instance, the IP addresses 192.168.1.0 and 192.168.0.0 belong to different class C networks within the classful architecture. However, since the class C subnet mask was fixed as 255.255.255.0, a network administrator could not combine both networks.

Working of CIDR:

CIDR enables network routers to direct data packets to destination devices based on the specified subnet. Rather than the IP address being categorized based on classes, the network and host addresses are retrieved by the routers as directed by the CIDR suffix.

To learn how CIDR works, let's understand more about **CIDR blocks** and **CIDR notation**.

CIDR Blocks:

CIDR blocks are collections of IP addresses sharing a single network prefix and the same number of bits. A large block would feature a small suffix and more IP addresses.

The Internet Assigned Numbers Authority (IANA) allocates large CIDR blocks to regional internet registries (RIR). The next step is the RIR allocating smaller blocks to local internet registries (LIR), after which the LIR allocates them for enterprise use. Private users can submit applications for CIDR blocks to their internet service providers (ISPs).

CIDR represents IP addresses in binary. CIDR blocks are a core component of CIDR as they enable address groups to be put together and addressed as a single entity for routing functions. These blocks feature a sequence of bits shared by several IP addresses, known as the prefix. The network portion of the IP addresses is determined by the prefix.

For IPv4, CIDR block identification uses a syntax similar to IPv4 addresses. This syntax includes a dotted-decimal address, such as 192.168.0.0. The address is then followed by a slash and a number between 0 and 32 (e.g., /26). The number added after the slash specifies the prefix length, indicating the number of shared bits in the binary representation of the IP addresses.

CIDR blocks can represent a range of IP addresses. For example, a block with a 20-bit prefix is represented by a /20 CIDR block, and the exact addresses within that block may be different. The address segment in the CIDR notation can be skipped when focusing on network size.

Let's say a specific IP address is contained within a certain CIDR block. If the initial bits of the address are the same as the CIDR prefix, this address is said to match the CIDR prefix. The number of matching bits determines network size. While shorter CIDR prefixes are a match for more addresses, fewer addresses match longer prefixes.

CIDR blocks are also used for Internet Protocol Version 6 (IPv6) addresses, which feature a greater number of bits. However, the semantics and syntax for IPv6 CIDR blocks are the same as in IPv4. For IPv6, the prefix length can range between 0 and 128, indicating the number of shared bits in the address.

Certain CIDR prefixes have particular uses. For instance, point-to-point links between routers for security and policy applications use /127 prefixes. Subnets generally have a fixed 64-bit host identifier on broadcast MAC layer networks.

CIDR blocks play a fundamental role in IP addressing and routing. They enable efficient management and grouping of IP addresses, simplifying the handling of routing decisions by routers.

CIDR Notation:

A CIDR notation makes IP address representation simple and enhances the efficiency with which network administrators can organize and allocate IP addresses. The CIDR notation represents an IP address along with a suffix indicating network identifier bits in a particular format. For instance, 192.168.1.0 using a 22-bit network identifier can be expressed as 192.168.1.0/22.

Simply put, CIDR notation allows users to understand IP addresses and network masks more easily. Created by Phil Karn in the 1980s, the format used for CIDR notation consists of the IP address, a 'forward slash' character, and a number representing the count of consecutive '1-bits' in the network mask (also known as the network prefix). The IP address in CIDR notation follows the standards for either IPv4 or IPv6, while the number after the slash signifies the number of bits used to identify the network.

A CIDR notation can signify a specific address on a device or even the starting address of an entire network. For instance, an IP address 10.0.0.1 with a network prefix of 8 bits is represented by 10.0.0.1/8, while 10.0.0.0/8 can be used to indicate the beginning address for the whole network. A CIDR notation without an IP address can be used to signify a generic IPv4 network; for instance, a network with a 24-bit prefix and 8-bit host numbers can be signified using '/24'.

Here are a few examples that will help you understand CIDR notation better:

- The 1024 IPv4 addresses from 198.51.100.0 to 198.51.103.255 are represented by the IPv4 block 198.51.100.0/22.
- The block of IPv6 addresses from 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff is represented by IPv6 block 2001:db8::/48.
- The IPv6 loopback address is represented by ::1/128. Here, the prefix length (number of bits in the address) is 128.

After CIDR's introduction, CIDR notation gained popularity for IPv4. Network administrators found it easier to understand and compute the network prefix using a single number, such as 192.24.12.0/22, than the older dotted-decimal subnet mask format.

The formula **2^(address length – prefix length)** can be used to compute the number of addresses in a network or subnet. For instance, an IPv4 prefix length of /29 would have 2^(32-29) = 2^3 = 8 addresses within the subnet.

Benefits of CIDR:

With CIDR, enterprises enjoy greater flexibility in assigning IP addresses and routing data between devices.

1. Decreased IP Address Space Wastage: CIDR provides users flexibility while determining the network assignment and host identifier on an IP address. CIDR can be used to provision the needed number of IP addresses for a specific network and thus decrease wastage. Apart from this, CIDR minimizes routing table entries and streamlines data packet routing.

2. Swift Data Transmission: CIDR enables routers to classify IP addresses into several subnets efficiently. Enterprises can also swiftly create and group numerous subnets together. As such, data can be transmitted to its destination address without deviating from unnecessary paths.

3. VPC Creation: A virtual private cloud (VPC) is a digital space with controlled access hosted within a cloud environment. VPCs enable enterprises to provision workloads within secure, isolated environments. In the case of VPCs, CIDR IP addresses are used during the transfer of data packets among connected devices.

4. Flexible Supernet Deployment: A supernet is a collection of subnets that share similarities in network prefixes. CIDR allows for the flexible creation of supernets, which is not possible through conventional masking architecture. For instance, an enterprise could combine IP addresses into a single network block through a notation such as:

192.168.1 /23

192.168.0 /23

A subnet mask of 255.255.254.0 is applied to the IP address through this notation. Thus, the first 23 bits are returned as the network address. The router would require only a single routing table entry for data packet management between devices on the subnets.

Drawbacks of CIDR:

While CIDR brings numerous advantages to IP address management, it is not without its limitations and potential challenges.

1. Complexity: Implementing and managing CIDR is generally more complex than traditional class-based addressing. Often, it requires additional training and experience among network administrators.

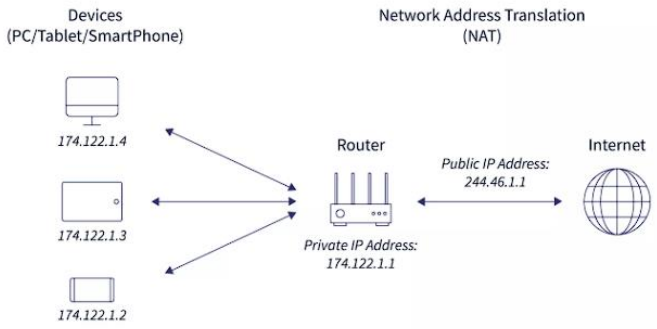
2. Compatibility: Certain older network devices are incompatible with CIDR. In larger networks, this could translate to difficulties and additional costs when transitioning to a CIDR-powered network.

3. Security: Without the right expertise, CIDR might increase the difficulty of implementing security measures such as access control lists and firewall rules. This has the potential to increase cybersecurity risks at the enterprise level.

Network Address Translation (NAT):

Network Address Translation (NAT) is a process of assigning a unique public IP address to represent an entire group of computers. In Network Address Translation, a network device, typically a router or NAT firewall—assigns a public address to one or more devices connected to a private network. Network address translation enables a single device to serve as an agent or intermediate between a local, private network and the internet, a public network. The basic objective of NAT is to reduce the number of public IP addresses in use for security and financial reasons.

NAT can help in this situation. A single device, such as a router, can be an intermediary between a local network and the internet. This implies that a single, distinctive IP address can represent a group of computers. To understand the NAT concept more significantly, we must know the inside and outside addresses.



The Inside address refers to the addresses that must be translated. Outside addresses are those that are not under the authority of a company. These are the network addresses where the address translation will take place. Let's look at the various types of inside and outside addresses. Let's have a look at the different types of inside and outside addresses -

- **Inside local address:** An IP address that is assigned to a host on the Inside (local) network. The address is most likely not an IP address issued by the service provider, instead, these are private IP addresses. This is the inside host, as seen from the inside network.
- **Inside global address:** The IP address that is used to represent one or more internal local IP addresses to the outside world. This is the inner host as perceived from the outside network.
- **Outside local address:** Outside local address is the actual IP address of the destination host on the local network after translation.
- **Outside global address:** From the outside network, this is how the external host appears. It is the original IP address of the external destination host.

How Does NAT Work?

NAT enables a single device, such as a **NAT firewall**, **NAT router**, or other network address translation device, to act as an intermediate between public and private networks—the internet and any local networks. This allows an entire group of devices to be represented by a unique IP address when interacting with the internet.

NAT works just like a company receptionist, which works based on a set of instructions given by the owner. The owner can tell the receptionist when he will be available and which client request must be forwarded and which one is blocked. The client calls the company's main number because the public number is known to everyone and demands that he wants to talk to the company's owner. Then based on the set of instructions given by the owner, the receptionist will now decide whether to forward the call or make the client wait. The receptionist will also decide where to forward the client's request based on your instructions.

Similar concepts apply to network address translation. The request comes at the public IP address and port, and the NAT instructions direct it to the proper location without disclosing the destinations' private IP addresses. NAT also translated the private IP of a machine into a unique IP address to allow communication of the local network to the internet. NAT can handle any number of IP address requests with the help of the NAT translation table. The NAT device maintains the translation table to ensure that the correct device in the private network will get the data packet from the internet.

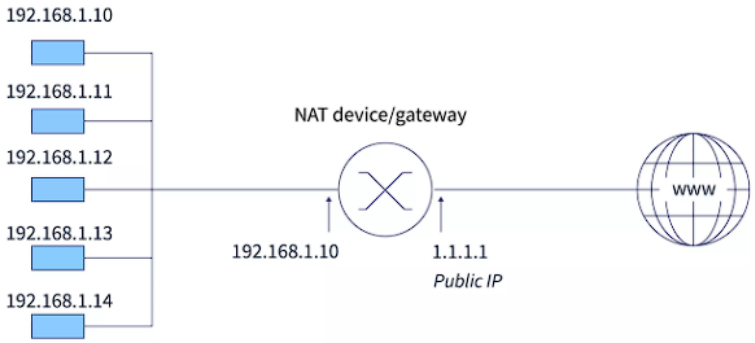
Assume two hosts, A and B are connected in a network. Now, both request the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT translates IP addresses, then when their packets arrive at the NAT, both of their IP addresses will be masked by the network's public IP address and delivered to the destination. Destination will send replies to the router's public IP address. As a result, when NAT receives a response, it will be unclear which response belongs to which host

(because source port numbers for both A and B are the same). To avoid this issue, NAT conceals the source port number and creates an entry in the NAT table.

NAT (Network Address Translation) Examples:

When a host on the internal or private network with an internal IP address needs to communicate with a device outside of the private network, it will use the public IP address on the network's gateway to identify itself to the outside world, and NAT would translate the private IP address into the public address. If, for instance, a computer with the internal address 192.168.1.10192.168.1.10 wished to communicate with a web server on the internet, NAT would translate that address to the company's public address, which we'll name in this case 1.1.1.11.1.1.1.

So that when communicating with the outside world, the internal address is recognized as the public address. This is necessary because, for the webserver to respond to this internal computer, it would need to transmit the response to the public address, which is a distinct and routable address on the internet. The private address is secret, non-routable, and concealed from the outside world, the original address of 192.168.1.10192.168.1.10 cannot be used. The public address for that company would be this one at 1.1.1.11.1.1.1, which is visible to everyone.



Network Address Translation

The web server would now respond to that 1.1.1.11.1.1.1 public address. NAT would use its records to convert the packets received from the web server intended for 1.1.1.11.1.1.1 back to the internal network address of 192.168.1.10192.168.1.10 so that the computer that requested the original information would get the requested packets.

The two advantages of NAT are now readily apparent. First, it would reduce the number of IP addresses we need because not every computer needs a public address. Second, it would shield these private computers from prying eyes. Only the public address is visible to everyone, everything else is concealed behind it. Therefore, nothing past the public address on the firewall's or router's external interface may be seen from the internet.

What are Network Address Translation (NAT) Types?

There are generally three types of NAT, and these are mentioned below.

1. Static NAT:

In this, one **unregistered** (Private) IP address is mapped to one legally **registered** (Public) IP address or local and global addresses are mapped one to one. Usually, this is utilized for hosting websites. Since numerous devices need an internet connection and a public IP address is required to give Internet access, these are not used in enterprises. Suppose if, 2000 devices require internet access, the company will need to purchase 2000 public addresses, which will be highly expensive.

2. Dynamic NAT:

An unregistered IP address is converted into a **registered** (Public) IP address using a pool of public IP addresses in this sort of NAT. The packet will be dropped if the pool's IP address is not free since only a predetermined number of private IP addresses can be converted to public addresses.

Consider that only two private IP addresses can be translated at any given time if there is a pool of two public IP addresses. Many private IP addresses are mapped to a pool of public IP addresses because the packet will be dropped if a third private IP address tries to access the internet. When a set amount of users need to access the Internet, NAT is utilized. The company must purchase numerous international IP addresses to create a pool, which is also highly expensive.

3. Port Address Translation (PAT):

It is also known as NAT overload. This allows for converting numerous **local** (private) IP addresses to a single registered IP address. Port numbers are employed to identify the traffic or which traffic comes from which IP address. Since thousands of individuals can access the internet using just one genuine **global** (public) IP address, this is the most widely utilized method.

Advantages of Network Address Translation:

- NAT connects various hosts to the global internet using a smaller number of public (external) IP addresses, thereby conserving IP address space.
- NAT keeps internal addresses hidden from the outside network and improves security for private networks.

- Network Address Translation provides a private **IPv4** addressing scheme and avoids modifying your internal addresses if your service provider changes.
- Adding a new client to the local network environment with NAT is simpler since local devices are privately addressed.
- In terms of setting up any network, NAT provides network flexibility.
- The use of NAT significantly decreases the cases of address overlapping.

Disadvantages of Network Address Translation:

- NAT uses a lot of memory since it transforms local and global IP addresses and stores the result in memory.
- NAT is not highly scalable so it doesn't perform well at a higher scale.
- Some applications have some compatibility issues with NAT.
- As NAT converts the IP addresses so, this conversion may be time-consuming.
- NAT complicates tunneling protocols such as IPsec.

Basics of IP Support Protocols:

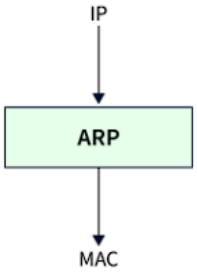
Basic IP Support Protocols are essential components of the modern Internet infrastructure that facilitate efficient communication and data transfer across networks. These protocols play a crucial role in establishing and maintaining connections between devices, enabling the seamless exchange of information. Understanding these fundamental protocols is essential for network administrators, engineers, and anyone involved in managing and troubleshooting network connectivity.

IP, or Internet Protocol, serves as the backbone of the Internet, responsible for addressing and routing packets of data between devices. However, the successful transmission of data relies on additional support protocols that address various aspects of network communication. Basic IP Support Protocols encompass a range of protocols that assist in tasks such as host configuration, error detection and correction, and network management.

ARP:

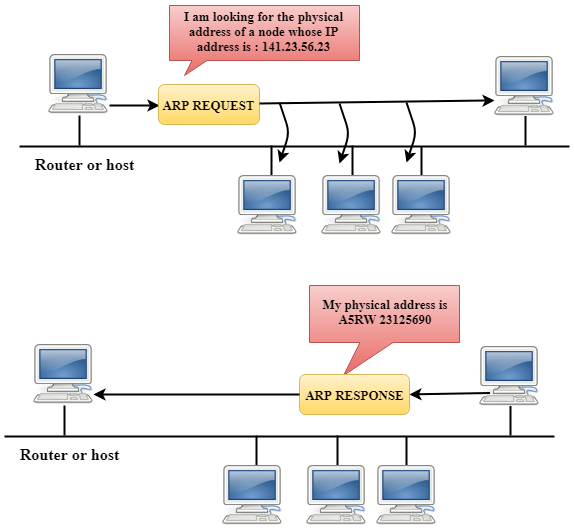
- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

Note: MAC address: The MAC address is used to identify the actual device. IP address: It is an address used to locate a device on the network.



How ARP works:

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.

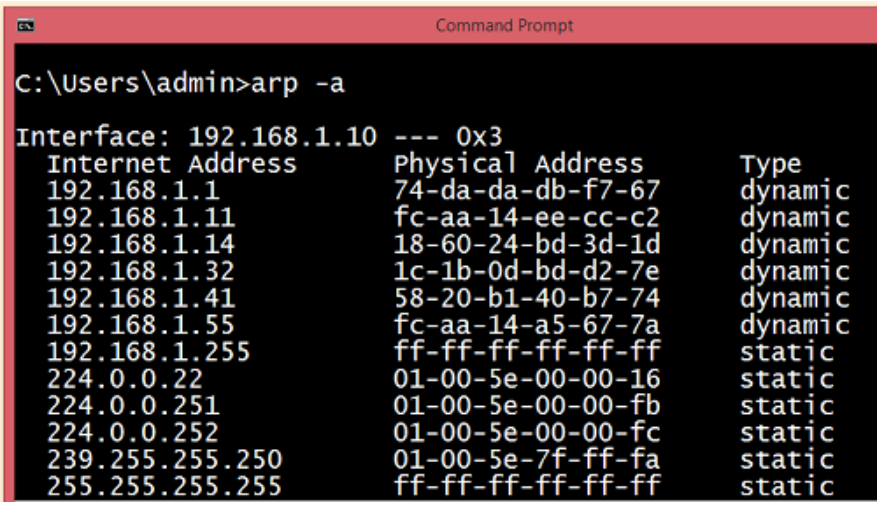


Steps taken by ARP protocol:

If a device wants to communicate with another device, the following steps are taken by the device:

- The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.

- If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
- The device that has the matching IP address will then respond back to the sender with its MAC address
- Once the MAC address is received by the device, then the communication can take place between two devices.
- If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.



Note: ARP cache is used to make a network more efficient.

In the above screenshot, we observe the association of IP address to the MAC address.

There are two types of ARP entries:

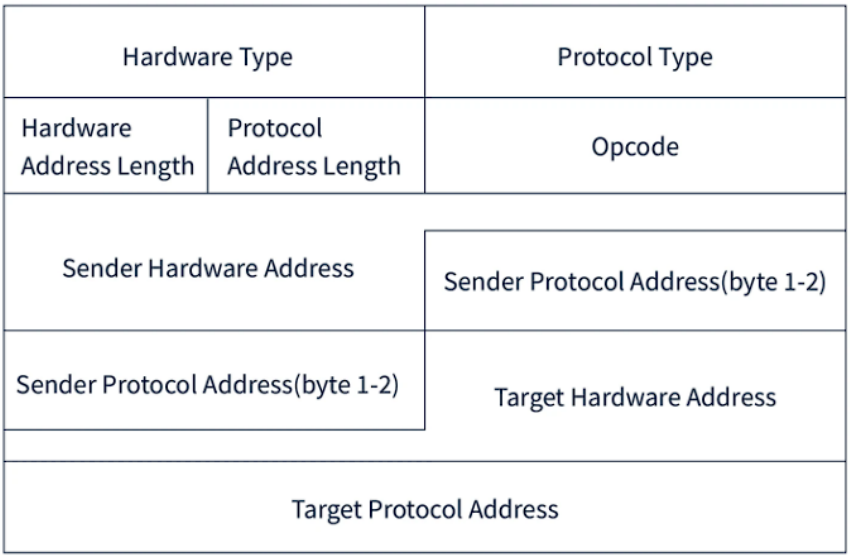
- **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
- **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.

ARP Terms:

- **ARP Cache:** After resolving the MAC address, the ARP sends it to the cache stored in a table to use in the future. The following communications can use the MAC address from the table.
- **ARP Cache Timeout:** The time for which the MAC address in the ARP cache can reside.
- **ARP request:** The broadcasting of a packet over the network to validate whether it reaches to the destination MAC address or not. The broadcasting of the packet is called an ARP request.
- **ARP response/reply:** The MAC address response that the source receives from the destination aids in further communication of the data. This response is called the ARP response.

ARP Packet Structure:

Following are the components of the ARP packet format:



1. Hardware Type: This is for specifying the type of hardware being used in the local network to transmit the Address Resolution Protocols message.

2. Protocol Type: This field is assigned a fixed number. For an instance, IPV4 has 2048.

3. Hardware Size: This represents the length of the MAC address in bytes. For example, the ethernet has a 6 bytes long MAC address.

4. Protocol Size: It represents the length of the IPV4 logical address, which generally is 4 bytes long.

5. OpCode: This is the length of the logical address in bytes. It indicates the nature of the ARP message. An ARP reply message holds the value of 2, while an ARP Request message is assigned the value of 1.

6. Sender MAC address: The hardware MAC address of the source device.

7. Sender IP address: The network layer address of the source device.

8. Target MAC address: This field works only during the reply phase and does not hold any value during the request phase. It stores the hardware MAC address of the receiver device.

9. Target IP address: The network layer address of the receiver device.

Types of Address Resolution Protocols:

Address Resolution Protocol is of the following four types:

1. Proxy ARP:

A Layer 3 device can reply to an ARP request for a target that is on a different network than the sender by using a technique called proxy ARP. In response to the ARP, the router that has been set for Proxy ARP maps its MAC address to the target IP address, deceiving the sender into believing that the message has arrived at destination.

Because the packets have the required information, the proxy router at the backend forwards them to the correct location.

2. Gratuitous ARP:

The host's ARP request known as "gratuitous ARP" aids in locating duplicate IP addresses. This is a broadcast request for the router's IP address. All other nodes are unable to use the IP address assigned to a switch or router in the event that it sends out an ARP request to obtain its IP address and receives no ARP answers in return. However, another node uses the IP address assigned to the switch or router if it sends an ARP request for its IP address and gets an ARP response.

3. Reverse ARP (RARP):

In a local area network (LAN), the client system uses this networking protocol to ask the ARP gateway router table for its IPv4 address. The network administrator creates a table in the gateway-router that is used to correlate the IP address with the MAC address.

4. Inverse ARP (InARP):

The purpose of inverse ARP, which is the opposite of ARP, is to deduce the nodes' IP addresses from their data link layer addresses. Frame relays and ATM networks, where Layer 2 virtual circuit addressing is frequently obtained from Layer 2 signalling, are the primary applications for them. These virtual circuits can be used with the necessary Layer 3 addresses accessible.

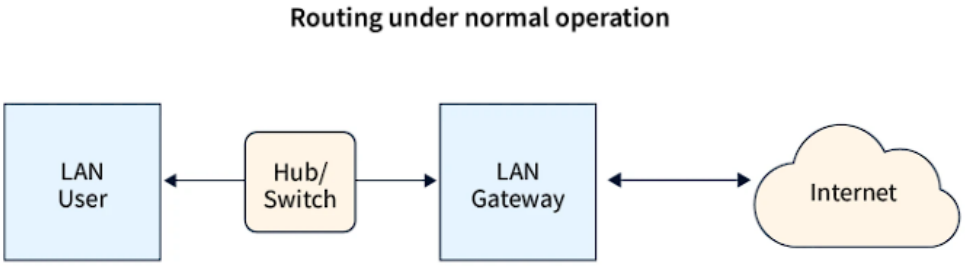
What is ARP Spoofing?

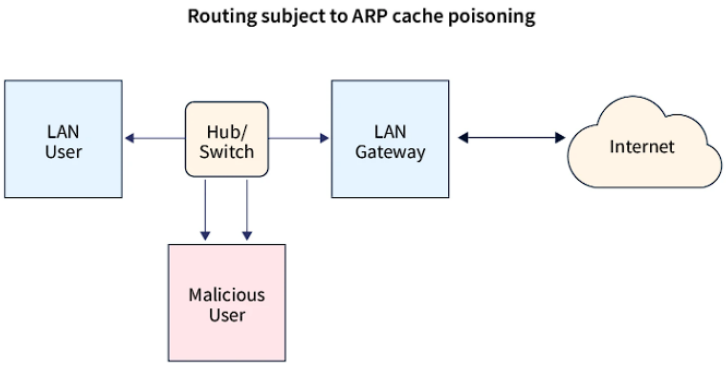
ARP spoofing is also referred to as ARP cache poisoning and ARP poison routing. It is a technique using which an attacker sends a spoofed Address Resolution Protocol message onto a LAN. Usually, the goal is to associate the MAC address with the IP address of some other host (the default gateway, etc). This leads to any traffic meant for that IP address being sent to the attacker instead.

ARP cache poisoning enables an attacker to modify the traffic, intercept data frames on a network, stop all traffic, etc. Often the ARP spoofing attacks are used as a means of opening a window for other attacks, such as man in the middle, denial of service (D.O.S.), session hijacking attacks, etc. The attack affects only networks that use ARP. Also, it is required that the attacker possesses direct access to the targeted local network segment.

How to Avoid ARP spoofing?

- Using static ARP tables.
- Taking secure managed Ethernet switches.
- Controlling physical access to the place of business.
- Isolating the network by concentrating all the important resources in a dedicated network segment.
- Encryption reduces the severe damage caused by ARP spoofing.





History and Future of ARP:

The address resolution was an issue significant from the very start of the development of the TCP/IP model. A large early part of the development of IP was conducted on the then-fledgling Ethernet LAN technology (even before Ethernet was officially standardized as IEEE 802.3). It became essential to create a way to map IP addresses to Ethernet addresses for enabling communication over Ethernet networks.

There were observed two possible methods: direct mapping and dynamic resolution. But since IP addresses are only 32 bits long while Ethernet addresses are 48 bits long, thus direct mapping was immediately ruled out. Thus was developed the TCP/IP Address Resolution Protocol (ARP), which is described in one of the earliest of the Internet RFCs still in common use: RFC 826, An Ethernet Address Resolution Protocol, published in 1982.

Since ARP was genuinely developed for Ethernet, it denotes a nexus between the most popular layer three internetworking protocol and layer two LAN protocol, even today, two decades later. But it was realized that even if Ethernet was a common way of transporting IP, it may not turn out to be the only one. Thus ARP was set as the general protocol.

128 bits long IPv6 addresses use the Neighbor Discovery protocol instead of ARP, for acquiring the configuration information. Even though less common as compared to IPV4, the use of IPv6 is increasing. Neighbor Discovery works in the second layer of the OSI reference model. For discovering the neighboring nodes, it uses Internet Control Message Protocol 6.

Alternatives to ARP:

Instead of ARP, the IPv6 protocol utilizes the NDP (Neighbor Discovery Protocol) and its extensions (Secure Neighbor Discovery, etc). Instead of using an active protocol, computers maintain lists of known addresses. In NDP, every system maintains a database of the Layer 3(IP addresses, etc) to Layer 2 (Ethernet MAC addresses, etc) address mappings.

This database id primarily maintained by interpreting the ARP packets from the local network link. For the same reason, it is also referred to as the ARP cache. In early times, in order to maintain the mapping between addresses, other methods were used, for example centrally maintained lists, static configuration files, etc.

ARP Stuffing:

ARP Stuffing means a user “stuffing” a static ARP entry into their local computer system's ARP cache, with the desired IP address of the device they want to configure. ARP stuffing can be used by networked cameras, networked power distribution devices, and other similar embedded systems which lack a user interface. It is used for making an initial network connection, although there is no involvement of any ARP protocol. ARP stuffing is a solution to a problem in network management of consumer devices, precisely the allocation of IP addresses of ethernet devices where:

1. The user is unable to control DHCP or other similar protocols.
2. The device does not possess a user interface to configure it.
3. The computer of the user is unable to communicate with it because it does not have a suitable IP address.

ARP stuffing, as a solution works as follows: an IP address is stuffed manually into the address table of the user’s computer system. Then special packets are sent to the device. Then the IP address is adopted by the device, and the user may then communicate with the device by web protocols or telnet for completing the configuration. Most of the time, such devices have a technique to shut this procedure once the device begins operating normally since it is susceptible to Denial-of-Service attacks.

ARP Relationship with DHCP and DNS and How Do They Differ?

Both ARP and DNS (Domain Naming System) are special protocols used for running the internet, but it's difficult to compare them. ARP is needed for packet transfers. DNS is not needed but reduces complexity. The Domain Name System is a decentralized and hierarchical naming system for resources connected with the network.

DHCP (Dynamic Host configuration protocol) is a network protocol. It is used for automatically assigning the IP address to a computer system or any other device on each LAN network. DHCP can use ARP. The RFC (Request For Comment) for DHCP mentions that when a device is offered an IP address by the DHCP server, the device can pass the address through to determine whether any other device on the network uses the address. If a conflict arises, the device must refuse the IP address offered and request an offer of a unique new address.

Address Resolution Methods:

Association between a protocol address and a hardware address is known as binding.

There are three techniques used for this purpose:

- **Table lookup** – Bindings stored in memory with protocol address as the key. It uses the data link layer to check the protocol address to find the hardware address.
- **Dynamic**–This type of network messaging method is used for "just-in-time" resolution. Data link layer sends message requests in a hardware address. destination responds.
- **Closed-form computation**–In this method, a protocol address is based on a hardware address. Data link layer derives the hardware address from the protocol address.

Advantages of using ARP:

- If you are using ARP, then MAC addresses can easily be known if you know the IP address of the same system.
- End nodes should not be configured to "know" MAC addresses. It can be found when needed.
- ARP's goal is to enable each host on a network that allows you to build up a mapping between IP addresses and physical addresses.
- The set of mappings or table stored in the host is called ARP table or ARP cache.

Dynamic Host Configuration Protocol (DHCP):

Any device or node on a network can receive a dynamic IP address through the **Dynamic Host Configuration Protocol** (DHCP), a network administration protocol (Internet Protocol). These setups are automated and centrally managed using DHCP. New devices don't require manual IP address assignment. Therefore, connecting to a DHCP-based network does not require any user configuration.

Both small business networks and extensive enterprise networks can use DHCP. The majority of routers and networking hardware use DHCP by default. DHCP is often referred to as RFC 2131 (Request for comments).

A network DHCP server that is deployed centrally and client instances of the protocol stack on each computer or device make up the technology, which eliminates the necessity for manually configuring each network device individually. A client uses the DHCP protocol to ask the DHCP server for a set of parameters the first time they connect to the network and then regularly after that.

Networks of all sizes, including residential networks, sizable campus networks, and regional ISP networks, can use DHCP. The DHCP server functionality is available on a lot of routers and home gateways. The majority of home network routers get a special IP address inside the ISP network. A DHCP server assigns each device a local IP address within a local network.

Network managers would have to manually distribute IP addresses from the pool if **Dynamic Host Configuration Protocol** (DHCP) didn't exist, which would be unacceptably time-consuming, ineffective, and prone to error. Fortunately, DHCP is a real thing.

Why Use DHCP?

Dynamic Host Configuration Protocol (DHCP) offers several compelling reasons for its widespread adoption in networking:

1. **Automatic IP Address Assignment**: DHCP automates the process of assigning IP addresses to devices on the network. This eliminates the need for manual configuration of IP addresses on each device, saving time and reducing the likelihood of configuration errors.
2. **Efficient Resource Allocation**: DHCP efficiently manages IP address allocation by dynamically assigning addresses from a pool of available addresses. It ensures that IP addresses are only assigned to devices when they are needed, preventing wastage of IP address resources.
3. **Centralized Configuration**: DHCP allows centralized management of network configuration settings, such as IP addresses, subnet masks, default gateways, DNS server addresses, and other parameters. Administrators can configure DHCP servers to distribute consistent network settings to all devices on the network.
4. **Flexibility and Scalability**: DHCP is highly scalable and can accommodate networks of varying sizes, from small local networks to large enterprise networks. It supports the dynamic addition and removal of devices without manual intervention, making it suitable for dynamic and growing networks.
5. **Ease of Network Maintenance**: DHCP simplifies network maintenance tasks by enabling administrators to make configuration changes centrally on DHCP servers. Changes to network settings, such as IP address ranges or DNS server addresses, can be applied globally to all devices through DHCP server configuration updates.
6. **Reduced Configuration Errors**: By automating the assignment of network settings, DHCP reduces the likelihood of configuration errors that can occur when manually configuring network parameters on individual devices. This enhances network reliability and reduces troubleshooting efforts.

7. **Support for Mobile Devices**: DHCP is well-suited for environments with mobile or roaming devices, such as laptops, smartphones, and tablets. These devices can easily obtain network configuration settings from DHCP servers when connecting to different networks, eliminating the need for manual reconfiguration.

Components of DHCP:

1. **DHCP Server**: The DHCP server is a network device or software application responsible for managing and allocating IP addresses and other configuration parameters to DHCP clients. It maintains a pool of available IP addresses and leases them to clients upon request.
2. **DHCP Client**: A DHCP client is a device, such as a computer, smartphone, or network printer, that requests network configuration information from a DHCP server. When a client connects to a network, it sends a DHCP Discover message to discover available DHCP servers and obtain network settings.
3. **IP Address Pool**: The IP address pool is a range of IP addresses configured on the DHCP server for allocation to DHCP clients. When a client requests an IP address, the DHCP server assigns an available address from the pool.
4. **Lease Database**: The lease database is a storage mechanism used by the DHCP server to track the assignment of IP addresses to clients. It maintains records of leased IP addresses, lease durations, client identifiers (MAC addresses), and other lease-related information.
5. **Configuration Parameters**: DHCP servers can provide various network configuration parameters to DHCP clients, including:
    - IP address
    - Subnet mask
    - Default gateway (router)
    - Domain Name System (DNS) server addresses
    - Domain Name
    - Time Server
    - Network Time Protocol (NTP) server
    - Domain Name System (DNS) search list
    - Hostname

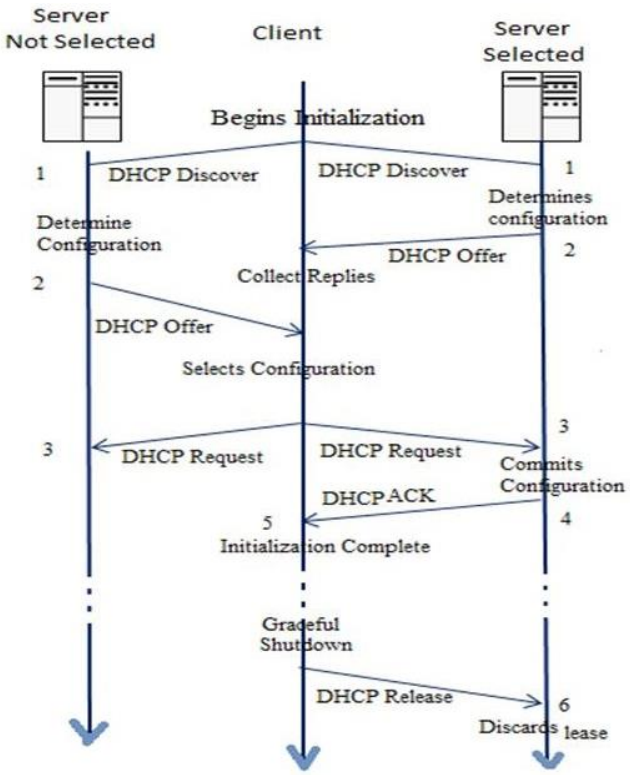
6. **DHCP Relay Agent**: In large networks with multiple subnets, a DHCP relay agent may be used to forward DHCP messages between DHCP clients and DHCP servers located on different subnets. The relay agent forwards DHCP Discover and Request messages to the DHCP server and relays DHCP Offer and Acknowledge messages back to the client.

The 8 DHCP Messages:

The DHCP (Dynamic Host Configuration Protocol) utilizes a series of messages exchanged between DHCP clients and servers to facilitate the automatic assignment of IP addresses and network configuration parameters. There are total of 8 DHCP messages involved in this process:

1. **DHCP Discover (Client-to-Server)**:
   - Sent by DHCP clients to discover available DHCP servers on the network.
   - Broadcast message requesting IP address assignment and network configuration parameters.
2. **DHCP Offer (Server-to-Client)**:
   - Sent by DHCP servers in response to DHCP Discover messages from clients.
   - Unicast message offering an IP address lease and network configuration parameters to the client.
   - Contains details such as the offered IP address, subnet mask, lease duration, and other configuration options.
3. **DHCP Request (Client-to-Server)**:
   - Sent by DHCP clients to request the offered IP address from a specific DHCP server.
   - Can be broadcast (in case of multiple DHCP offers) or unicast (when accepting a specific offer).
4. **DHCP Acknowledge (Server-to-Client)**:
   - Sent by the DHCP server to acknowledge the client's request for the offered IP address.
   - Unicast message confirming the IP address lease and providing other configuration parameters.
   - Indicates that the client can begin using the assigned IP address and network settings.

5. **DHCP Decline (Client-to-Server)**:
   - Optional message sent by a client to indicate that the offered IP address is already in use or invalid.
   - Helps prevent IP address conflicts by informing the server to retract the offer.
6. **DHCP Release (Client-to-Server)**:
   - Sent by DHCP clients to release their IP address lease back to the DHCP server.
   - Used when a client disconnects from the network or no longer requires the assigned IP address.
7. **DHCP Inform (Client-to-Server)**:
   - Optional message sent by DHCP clients to obtain additional configuration parameters from the DHCP server.
   - Used by clients that have already obtained an IP address but need to update or refresh configuration settings.
8. **DHCP NAK (Negative Acknowledge) (Server-to-Client)**:
   - Sent by DHCP servers to reject a client's DHCP Request message.
   - Indicates that the requested IP address is no longer available or invalid.
   - Prompts the client to restart the DHCP lease acquisition process.



Advantages of DHCP:

1. **Automatic Configuration**: Simplifies IP address assignment and network setup.
2. **Efficient Resource Allocation**: Dynamically assigns addresses, preventing wastage.
3. **Centralized Management**: Enables easy management of network settings.
4. **Flexibility and Scalability**: Adaptable to networks of varying sizes.
5. **Ease of Maintenance**: Streamlines network configuration updates.
6. **Reduced Errors**: Minimizes configuration mistakes, enhancing reliability.
7. **Support for Mobile Devices**: Facilitates seamless connectivity for mobile devices.

Disadvantages of DHCP:

1. **Dependency on Servers**: Network connectivity relies on DHCP server availability.
2. **Single Point of Failure**: Single DHCP server setup poses a risk of downtime.
3. **Lease Management**: Requires careful monitoring to avoid IP conflicts.
4. **Security Concerns**: Potential for malicious DHCP servers to compromise network security.
5. **Increased Traffic**: DHCP messages may impact network performance.
6. **IP Address Exhaustion**: Mismanagement can lead to IP address depletion.
7. **Limited Control**: Less control over specific IP address assignments.

Internet Control Message Protocol (ICMP):

A network device uses the Internet Control Message Protocol (ICMP) to diagnose network communication problems. Information about whether data is reaching its desired destination on time is primarily determined by ICMP. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is essential for error reporting and testing and it can also be used in distributed denial-of-service attacks.

Ping messages refer to both the ICMP echo request and echo reply messages. A network device receives an ICMP echo request from the ping command and immediately sends back an ICMP echo reply.

Additionally, it lacks a level within the Open Systems Interconnection (OSI) model, which outlines the seven layers involved with network transmissions. When you understand ICMP, you will see why it is such a valuable tool, but it is also important to comprehend how ICMP can be used in DDoS attacks that may threaten an organization.

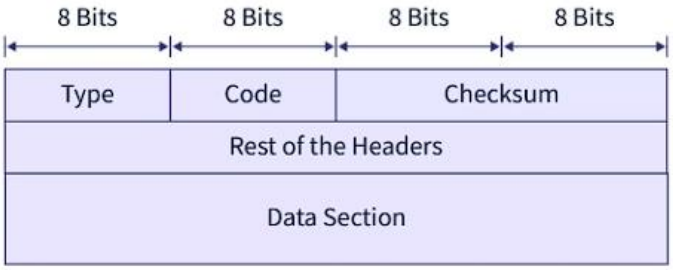
What is the Internet Control Message Protocol Used for?

- A network problem is diagnosed and reported using the Internet Control Message Protocol (ICMP). When data does not arrive as expected, ICMP sends a message from the sender to the receiver. Ping and traceroute use ICMP messages as part of the diagnostic process to provide information on how data is being transmitted.
- Some senders want to send a message to a destination, but the router is unable to do so. The router notifies the sender that I am unable to send the message to that destination.
- ICMP is also commonly used for network diagnostics. Both traceroute and ping use ICMP. Traceroute and ping are messages sent when data is successfully transmitted. The physical routers that handled the data are included.
- ICMP is also used to hurt network performance. ICMP floods, Smurf attacks, and ping of death attacks are used to overwhelm a device on the network and prevent it from functioning properly.

How Does ICMP Work?

- In ICMP, no connection is formed. The message is simply sent. In addition, unlike TCP and UDP, which specify the ports to which information is sent, ICMP does not specify a specific port to which information will be received.
- When the network disables the delivery of packets to the destination device, it generates and sends error messages to the sender device. Error messages include time exceeded, parameter problem, destination unreachable, network congestion, etc.
- An IP (Internet Protocol) datagram is sent from one device to another through multiple routers and intermediaries when it is sent from one device to. There can be an error in forwarding that IPV4 datagram. Hence, ICMP messages are divided into two broad categories: Error messages and Query messages

ICMP Message Format:



ICMP Message Format

So far, we've learned about two different forms of ICMP messages.

Let's look at the format of ICMP messages presently. The following is the format of the lower ICMP message:

Although the ICMP header differs for each message type, the first three fields are the same in all messages. These three fields take up a total of 4 bytes.

These fields are described in great detail:

- **Type:** This specifies the field message type. This field, for example, is used to establish the code associated with any form of an error report. Similarly, if there is a query message, this field will appear in the code for that query.

  Some common message types are as follows:

  - Type 0 – Echo reply
  - Type 3 – Destination unreachable
  - Type 5 – Redirect Message
  - Type 8 – Echo Request
  - Type 11 – Time Exceeded
  - Type 12 – Parameter problem
- **Code (8-bit):** For error messages, this defines a subtype of field error. For example, if a destination unreachable error occurs, the code field indicates what type of destination the error is. Examples: Network unreachable (code 0), host unreachable (code 1), protocol unreachable (code 2), etc. The code also defines the subtypes of these errors.
- **Checksum (16-bit):** Checksums are calculated from the headers and data used to detect errors. In IP datagrams, ICMP messages are included. The remaining IP headers can be seen in the ICMP message header section.
- **Data:** In the context of error messages, the package contains the complete information for the package in this section.

ICMP in DDoS Attacks:

In Distributed DOS (DDoS) attacks, attackers provide so much extra traffic to the target, so that it cannot provide service to users. There are so many ways through which an attacker executes these attacks, which are described below.

Ping of Death Attack: Whenever an attacker sends a ping, whose size is greater than the maximum allowable size, oversized packets are broken into smaller parts. When the sender re-assembles it, the size exceeds the limit which causes a buffer overflow and makes the machine freeze. This is simply called a Ping of Death Attack. Newer devices have protection from this attack, but older devices did not have protection from this attack.

ICMP Flood Attack: Whenever the sender sends so many pings that the device on whom the target is done is unable to handle the echo request. This type of attack is called an ICMP Flood Attack. This attack is also called a ping flood attack. It stops the target computer's resources and causes a denial of service for the target computer.

Smurf Attack: Smurf Attack is a type of attack in which the attacker sends an ICMP packet with a spoofed source IP address. These type of attacks generally works on older devices like the ping of death attack.

Types of ICMP Messages:

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation is needed and the DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect the datagram for the network
	1	Redirect datagram for the host
	2	Redirect the datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host

8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded.
12 – Parameter Problem	0	The pointer indicates an error.
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Disadvantages of ICMP:

- If the router drops a packet, it may be due to an error; but, because to the way the IP (internet protocol) is designed, there is no way for the sender to be notified of this problem.
- Assume, while a data packet is being transmitted over the internet, that its lifetime is over and that the value of the time to live field has dropped to zero. In this case, the data packet is destroyed.
- Although devices frequently need to interact with one another, there isn't a standard method for them to do so in Internet Protocol. For instance, the host needs to verify the destination's vital signs to see if it is still operational before transmitting data.