UNIT-4

Transport Layer2:

The principles behind connection oriented data transfer:

Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer. The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender. It is actually a data transfer method among two devices or computers in a different network.

This connection service is generally provided by protocols of both network layer (signifies different path for various data packets that belongs to same message) as well as transport layer (use to exhibits independence among packets rather than different paths that various packets belong to same message will follow).

Operations :
There is a sequence of operations that are needed to b followed by users. These operations are given below :

1. **Establishing Connection –**
   It generally requires a session connection to be established just before any data is transported or sent with a direct physical connection among sessions.
1. **Transferring Data or Message –**
   When this session connection is established, then we transfer or send message or data.
2. **Releasing the Connection –**
   After sending or transferring data, we release connection.

Different Ways :
There are two ways in which connection-oriented services can be done. These ways are given below :

1. **Circuit-Switched Connection –**
   Circuit-switching networks or connections are generally known as connection-oriented networks. In this connection, a dedicated route is being established among sender and receiver, and whole data or message is sent through it. A dedicated physical route or a path or a

circuit is established among all communication nodes, and after that, data stream or message is sent or transferred.

2. **Virtual Circuit-Switched Connection –**
   Virtual Circuit-Switched Connection or Virtual Circuit Switching is also known as Connection-Oriented Switching. In this connection, a preplanned route or path is established before data or messages are transferred or sent. The message Is transferred over this network is such a way that it seems to user that there is a dedicated route or path from source or sender to destination or receiver.

Types of Connection-Oriented Service :

Service	Example
Reliable Message Stream	Sequence of pages, etc.
Reliable Byte Stream	Song Download, etc.
Unreliable Connection	VoIP (Voice Over Internet Protocol)

Advantages :

- It kindly support for quality of service is an easy way.
- This connection is more reliable than connectionless service.
- Long and large messages can be divided into various smaller messages so that it can fit inside packets.
- Problems or issues that are related to duplicate data packets are made less severe.

Disadvantages :

- In this connection, cost is fixed no matter how traffic is.
- It is necessary to have resource allocation before communication.
- If any route or path failures or network congestions arise, there is no alternative way available to continue communication.

stop-and-wait:

Stop and Wait ARQ is a Sliding Window Protocol method used for the reliable delivery of data frames. The stop-and-wait ARQ is used for noisy channels or links to handle flow and error control between sender and receiver. The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver.

The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver. The ACK indicates that the receiver successfully received the data frame. After receiving the ACK from the receiver, the sender delivers the next data frame. So there is a stop before the next data frame is transferred, hence it is known as the Stop and Wait ARQ protocol.

Characteristics of Stop and Wait ARQ

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait for ARQ mainly implements the Sliding Window Protocol concept with Window Size 1

Useful Terms in Stop and Wait Protocol

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

Propagation Delay = *(Distance between routers) / (Velocity of propagation)*

- RoundTripTime (**RTT**) = Amount of time taken by a packet to reach the receiver + Time taken by the Acknowledgement to reach the sender
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 255 seconds)

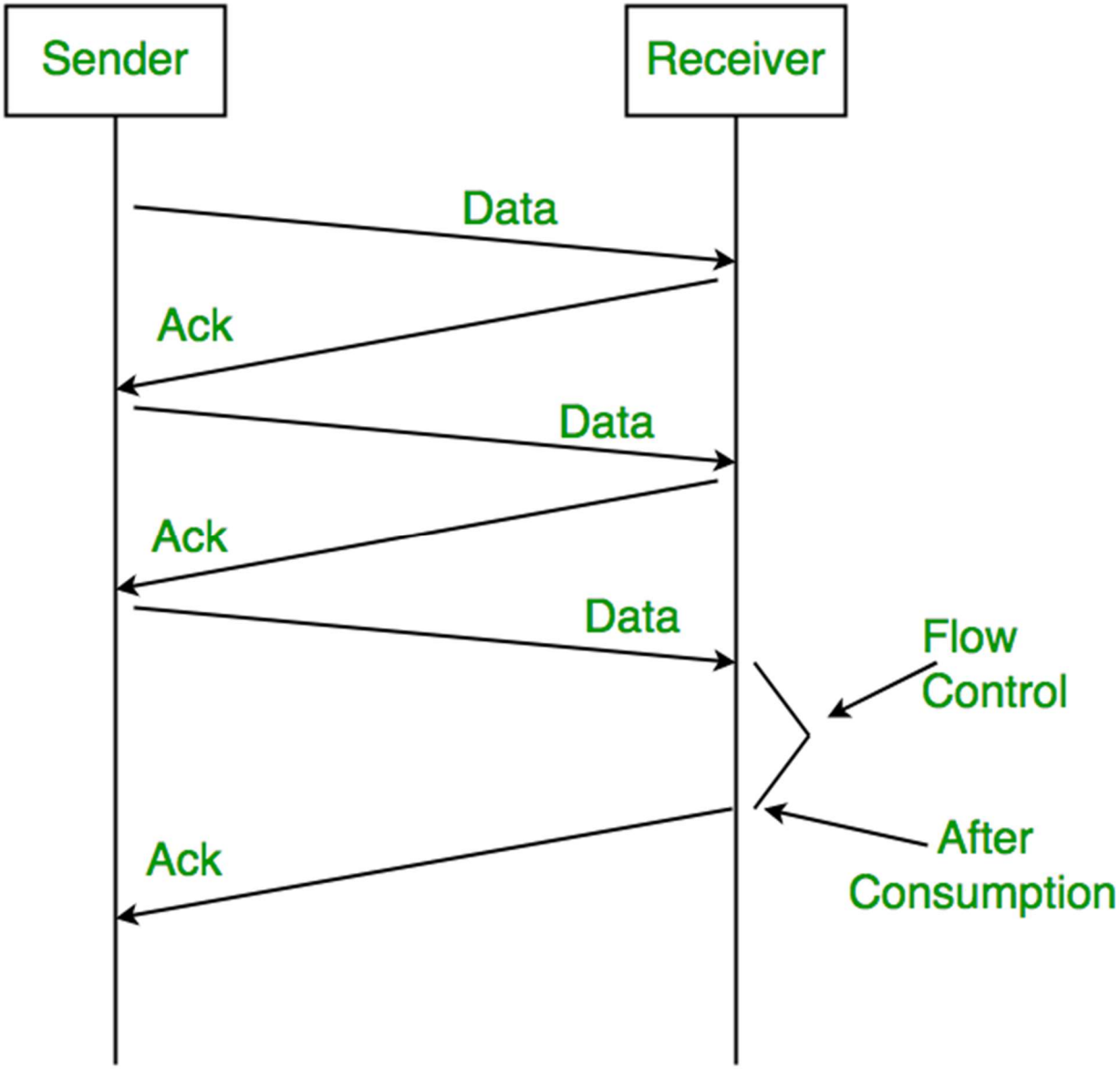
Simple Stop and Wait

At Sender

- Rule 1) Send one data packet at a time.
- Rule 2) Send the next packet only after receiving acknowledgment for the previous.

At Receiver

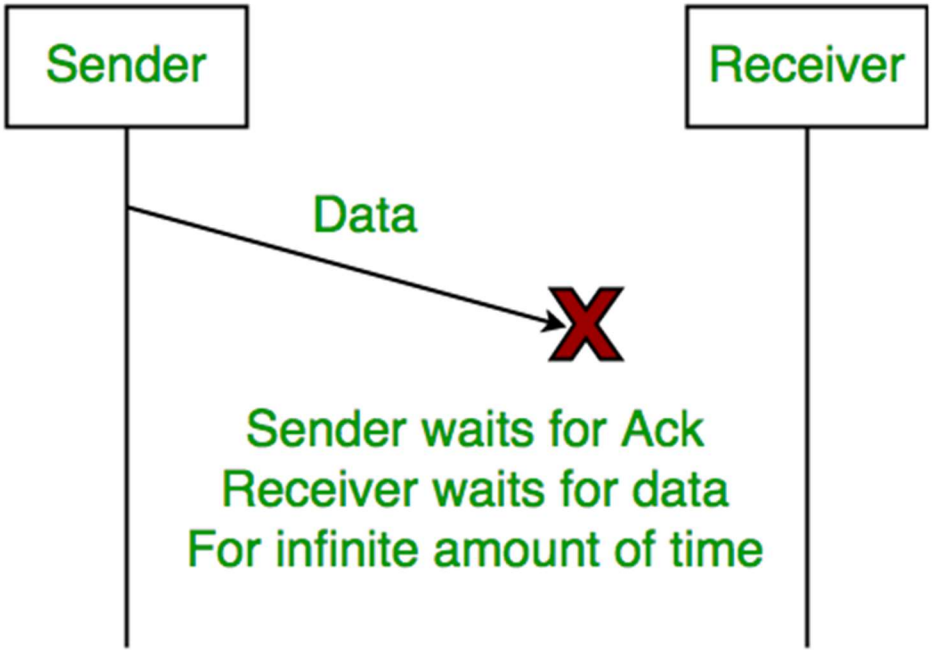
- Rule 1) Send acknowledgement after receiving and consuming a data packet.
- Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)



Problems Associated with Stop and Wait

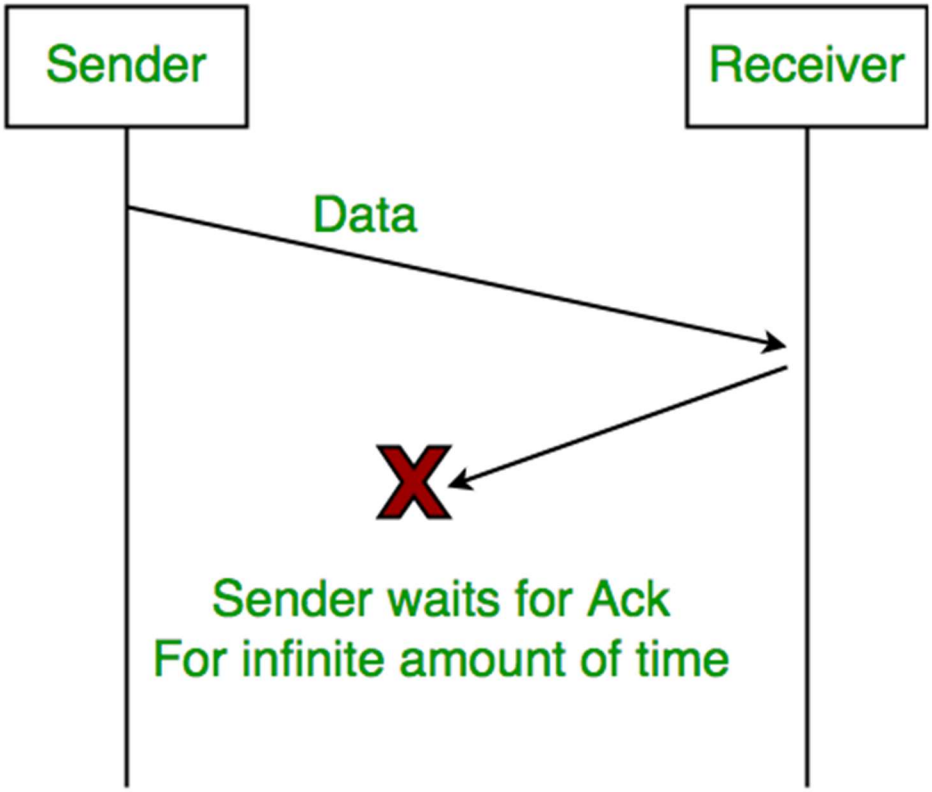
1. Lost Data

Assume the sender transmits the data packet and it is lost. The receiver has been waiting for the data for a long time. Because the data is not received by the receiver, it does not transmit an acknowledgment. The sender does not receive an acknowledgment, it will not send the next packet. This problem is caused by a loss of data.



2. Lost Acknowledgement

Assume the sender sends the data, which is also received by the receiver. The receiver sends an acknowledgment after receiving the packet. In this situation, the acknowledgment is lost in the network. The sender does not send the next data packet because it does not receive acknowledgement, under the stop and wait protocol, the next packet cannot be transmitted until the preceding packet's acknowledgment is received.

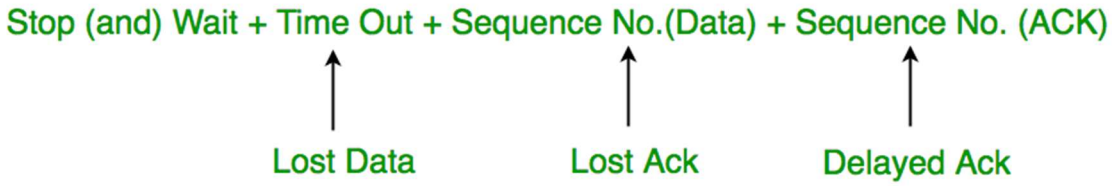


3. Delayed Acknowledgement/Data

Assume the sender sends the data, which is also received by the receiver. The receiver then transmits the acknowledgment, which is received after the sender's timeout period. After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait for ARQ (Automatic Repeat Request)

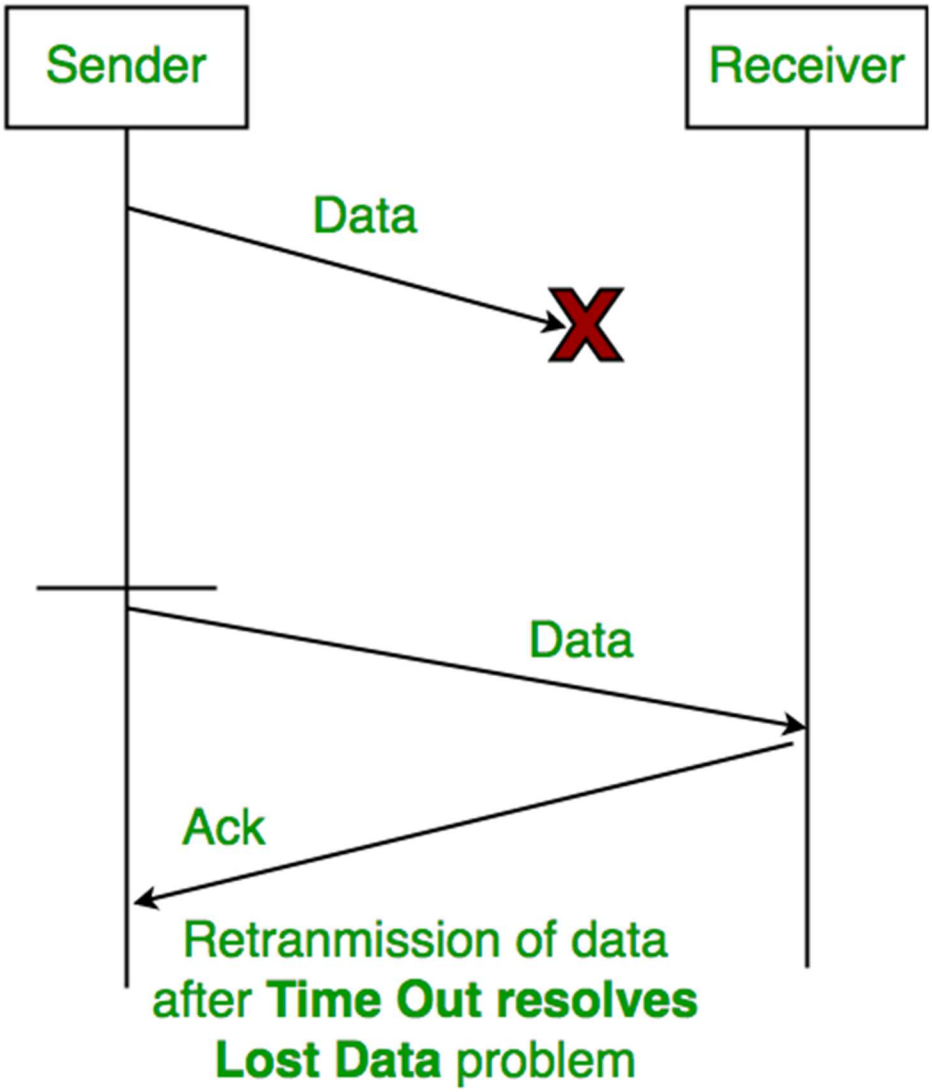
The above 3 problems are resolved by Stop and Wait for ARQ (Automatic Repeat Request) that does both error control and flow control.



1. Time Out

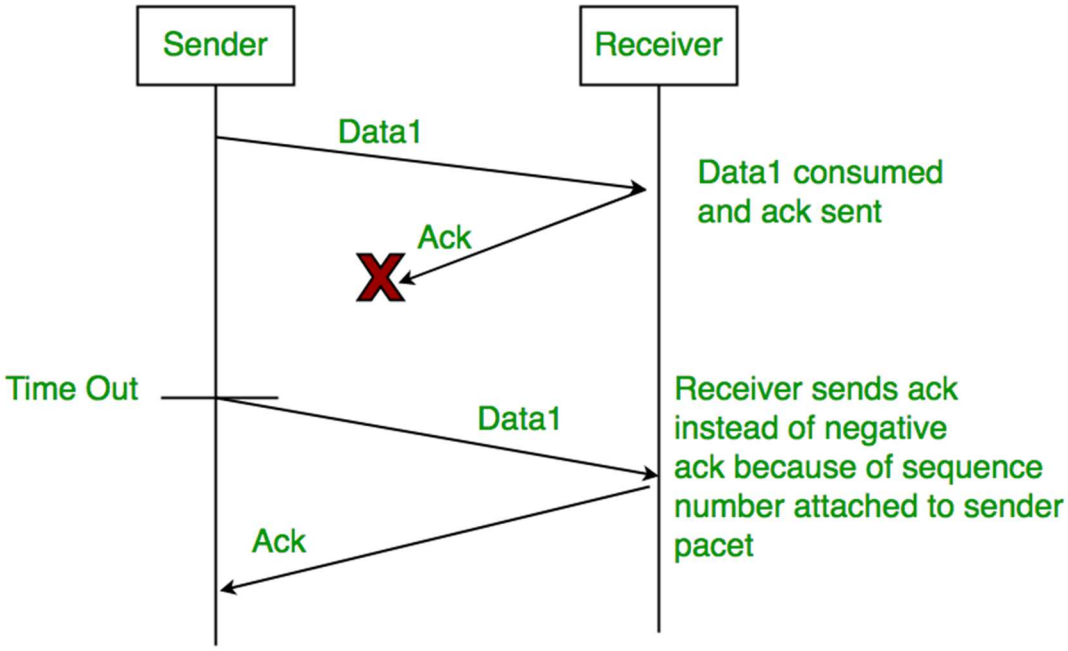
Timeout refers to the duration for which the sender waits for an acknowledgment (ACK) from the receiver after transmitting a data packet. If

the sender does not receive an ACK within this timeout period, it assumes that the frame was lost or corrupted and retransmits the frame.



2. Sequence Number (Data)

In Stop-and-Wait ARQ, the sender assigns sequence numbers to each data frame it sends. This allows the receiver to identify and acknowledge each frame individually, ensuring reliable delivery of data packets. After sending a frame, the sender waits for an acknowledgment before sending the next frame.



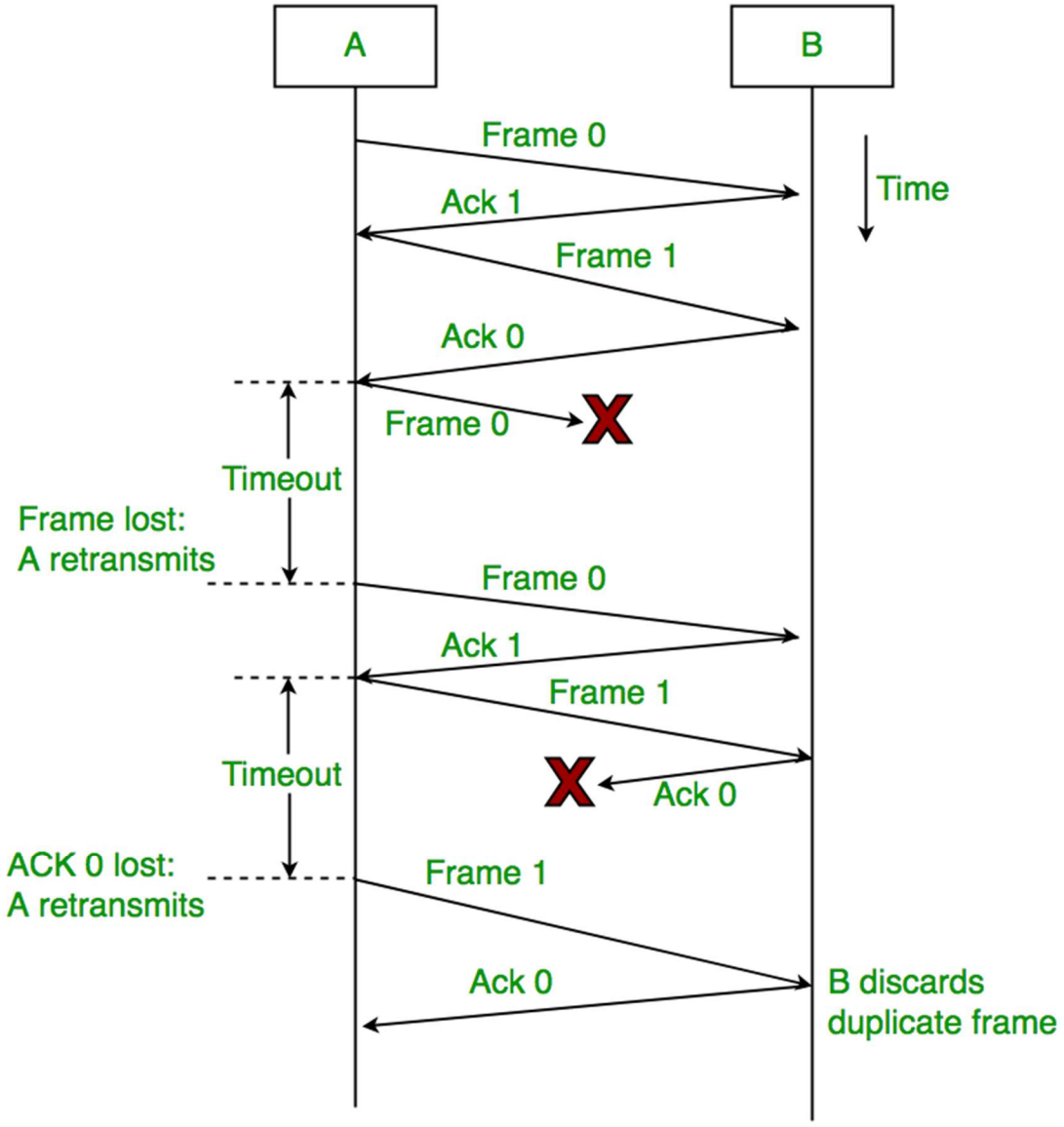
3. Sequence Number(Acknowledgement)

Similarly, sequence numbers are also used in acknowledgments (ACKs) sent by the receiver to acknowledge received data frames. When the receiver successfully receives a data frame, it sends an ACK back to the sender, indicating the sequence number of the next expected frame. The sender uses this ACK to determine whether the transmission was successful and whether it can proceed to send the next frame.

Working of Stop and Wait for ARQ

- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)

  There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ

- It uses a link between sender and receiver as a half-duplex link
- Throughput = 1 Data packet/frame per RTT
- If the Bandwidth*Delay product is very high, then they stop and wait for protocol if it is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example of "**Closed Loop OR connection-oriented** " protocols
- It is a special category of SWP where its window size is 1
- Irrespective of the number of packets sender is having stop and wait for protocol requires only 2 sequence numbers 0 and 1

Constraints in Stop and Wait ARQ

Stop and Wait ARQ has very less efficiency , it can be improved by increasing the window size. Also , for better efficiency , Go back N and Selective Repeat Protocols are used. The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country through a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence number. We will be discussing these protocols in the next articles. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections but performs badly for distant connections like satellite connections.

Advantages of Stop and Wait ARQ

- **Simple Implementation:** Stop and Wait ARQ is a simple protocol that is easy to implement in both hardware and software. It does not require complex algorithms or hardware components, making it an inexpensive and efficient option.
- **Error Detection:** Stop and Wait ARQ detects errors in the transmitted data by using checksums or cyclic redundancy checks (CRC). If an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, indicating that the data needs to be retransmitted.
- **Reliable:** Stop and Wait ARQ ensures that the data is transmitted reliably and in order. The receiver cannot move on to the next data packet until it receives the current one. This ensures that the data is received in the correct order and eliminates the possibility of data corruption.
- **Flow Control:** Stop and Wait ARQ can be used for flow control, where the receiver can control the rate at which the sender transmits data. This is useful in situations where the receiver has limited buffer space or processing power.
- **Backward Compatibility:** Stop and Wait ARQ is compatible with many existing systems and protocols, making it a popular choice for communication over unreliable channels.
-

Disadvantages of Stop and Wait ARQ

- **Low Efficiency:** Stop and Wait ARQ has low efficiency as it requires the sender to wait for an acknowledgment from the receiver before sending the next data packet. This results in a low data transmission rate, especially for large data sets.

- **High Latency:** Stop and Wait ARQ introduces additional latency in the transmission of data, as the sender must wait for an acknowledgment before sending the next packet. This can be a problem for real-time applications such as video streaming or online gaming.
- **Limited Bandwidth Utilization:** Stop and Wait ARQ does not utilize the available bandwidth efficiently, as the sender can transmit only one data packet at a time. This results in underutilization of the channel, which can be a problem in situations where the available bandwidth is limited.
- **Limited Error Recovery:** Stop and Wait ARQ has limited error recovery capabilities. If a data packet is lost or corrupted, the sender must retransmit the entire packet, which can be time-consuming and can result in further delays.
- **Vulnerable to Channel Noise:** Stop and Wait ARQ is vulnerable to channel noise, which can cause errors in the transmitted data. This can result in frequent retransmissions and can impact the overall efficiency of the protocol.

Go Back N AND Selective Repeat :

go-Back-N Protocol:

The Go-Back-N protocol is a sliding window protocol used for reliable data transfer in computer networks. It is a sender-based protocol that allows the sender to transmit multiple packets without waiting for an acknowledgement for each packet. The receiver sends a cumulative acknowledgement for a sequence of packets, indicating the last correctly received packet. If any packet is lost, the receiver sends a negative acknowledgement (NACK) for the lost packet, and the sender retransmits all the packets in the window starting from the lost packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer's timeout period, the sender retransmits all packets in the window.

The key features of the Go-Back-N (GBN) protocol include:

- Sliding window mechanism
- Sequence numbers
- Cumulative acknowledgements
- Timeout mechanism
- NACK mechanism
- Simple implementation.

Selective Repeat Protocol:

The Selective Repeat protocol is another sliding window protocol used for reliable data transfer in computer networks. It is a receiver-based protocol that allows the receiver to acknowledge each packet individually, rather than a cumulative acknowledgement of a sequence of packets. The sender sends packets in a window and waits for acknowledgements for each packet in the window. If a packet is lost, the receiver sends a NACK for the lost packet, and the sender retransmits only that packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer's timeout period, the sender retransmits only that packet.

key features include:

- Receiver-based protocol
- Each packet is individually acknowledged by the receiver
- Only lost packets are retransmitted, reducing network congestion
- Maintains a buffer to store out-of-order packets
- Requires more memory and processing power than Go-Back-N
- Provides efficient transmission of packets.

Similarities between the two protocols are:

- Both protocols use a sliding window mechanism to allow the sender to transmit multiple packets without waiting for an acknowledgement for each packet.
- Both protocols use sequence numbers to ensure the correct order of packets.
- Both protocols use a timer mechanism to handle lost or corrupted packets.
- Both protocols can retransmit packets that are not acknowledged by the receiver.
- Both protocols can reduce network congestion by only retransmitting lost packets.
- Both protocols are widely used in modern communication networks.

S.NO	Go-Back-N Protocol	Selective Repeat Protocol
1.	In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
2.	Sender window size of Go-Back-N Protocol is N.	Sender window size of selective Repeat protocol is also N.
3.	Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of selective Repeat protocol is N.
4.	Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
5.	In Go-Back-N Protocol, neither sender nor at receiver need sorting.	In selective Repeat protocol, receiver side needs sorting to sort the frames.
6.	In Go-Back-N Protocol, type of Acknowledgement is cumulative.	In selective Repeat protocol, type of Acknowledgement is individual.
7.	In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
8.	In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted.	In selective Repeat protocol, if Receives a corrupt packet, it immediately sends a negative

S.NO	Go-Back-N Protocol	Selective Repeat Protocol
		acknowledgement and hence only the selective packet is retransmitted.
9.	Efficiency of Go-Back-N Protocol is `N/(1+2*a)`	Efficiency of selective Repeat protocol is also `N/(1+2*a)`

TCP: Connection Establishment:

TCP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends.

Connection Establishment –
1. Sender starts the process with the following:

- **Sequence number (Seq=521):** contains the random initial sequence number generated at the sender side.
- **Syn flag (Syn=1):** request the receiver to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
- **Window size (window=14600 B):** sender tells about his buffer capacity in which he has to store messages from the receiver.

2. TCP is a full-duplex protocol so both sender and receiver require a window for receiving messages from one another.

- **Sequence number (Seq=2000):** contains the random initial sequence number generated at the receiver side.
- **Syn flag (Syn=1):** request the sender to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=500 B):** receiver tells its maximum segment size, so that sender sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.

Since $MSS_{receiver}$ < MSS_{sender}, both parties agree for minimum MSS i.e., 500 B to avoid fragmentation of packets at both ends.

```
Therefore, receiver can send maximum of 14600/500 = 29 packets.

This is the receiver's sending window size.
```

- **Window size (window=10000 B):** receiver tells about his buffer capacity in which he has to store messages from the sender.

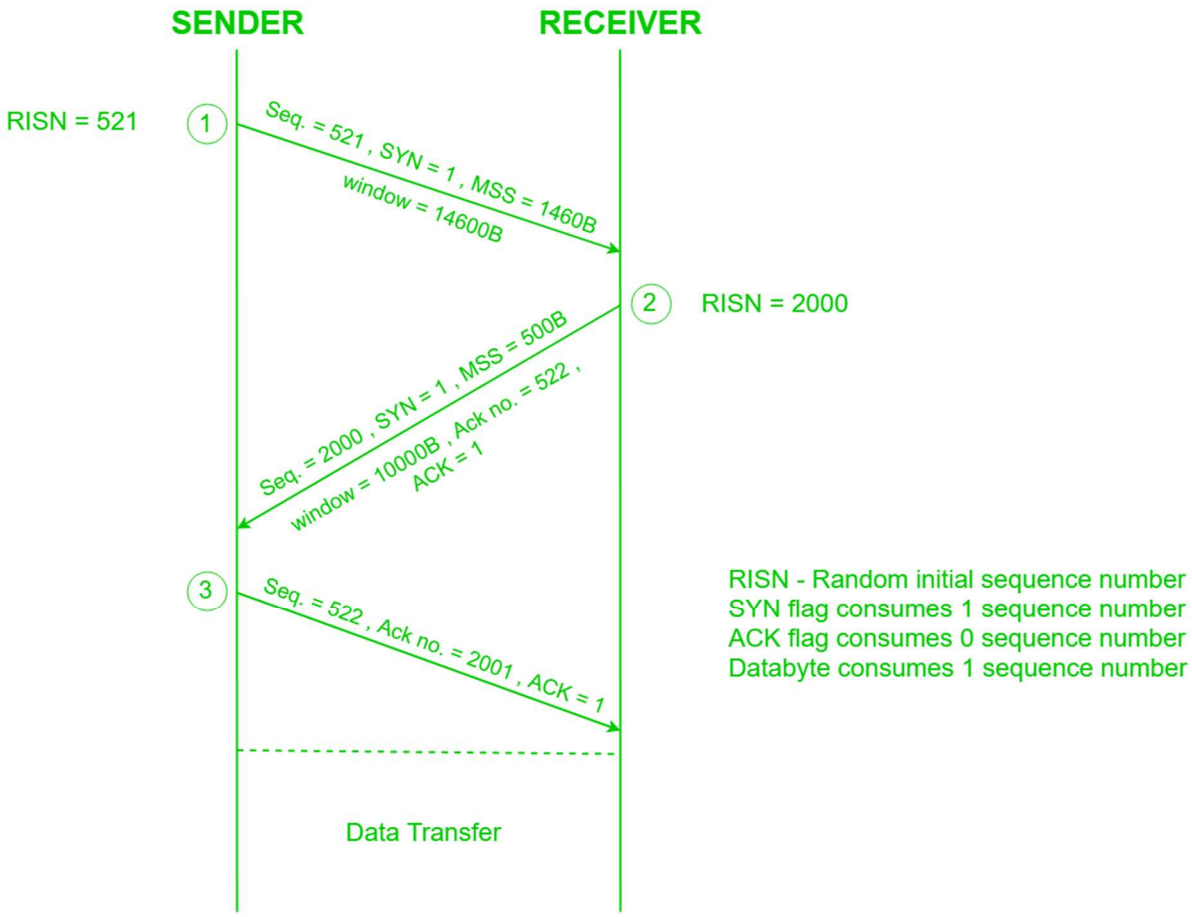
```
Therefore, sender can send a maximum of 10000/500 = 20 packets.

This is the sender's sending window size.
```

- **Acknowledgement Number (Ack no.=522):** Since sequence number 521 is received by the receiver so, it makes a request for the next sequence number with Ack no.=522 which is the next packet expected by the receiver since Syn flag consumes 1 sequence no.
- **ACK flag (ACk=1):** tells that the acknowledgement number field contains the next sequence expected by the receiver.

3. Sender makes the final reply for connection establishment in the following way:

- **Sequence number (Seq=522):** since sequence number = 521 in 1st step and SYN flag consumes one sequence number hence, the next sequence number will be 522.
- **Acknowledgement Number (Ack no.=2001):** since the sender is acknowledging SYN=1 packet from the receiver with sequence number 2000 so, the next sequence number expected is 2001.
- **ACK flag (ACK=1):** tells that the acknowledgement number field contains the next sequence expected by the sender.



Since the connection establishment phase of TCP makes use of 3 packets, it is also known as 3-way Handshaking **(SYN, SYN + ACK, ACK).**

TCP HEADER:

he various **services** provided by the TCP to the application layer are as follows:

1. **Process-to-Process Communication –**
   TCP provides a process to process communication, i.e, the transfer of data that takes place between individual processes executing on end systems. This is done using port numbers or port addresses. Port numbers are 16 bits long that help identify which process is sending or receiving data on a host.

2. **Stream oriented –**
   This means that the data is sent and received as a stream of bytes(unlike UDP or IP that divides the bits into datagrams or packets). However, the network layer, that provides service for the TCP, sends packets of information not streams of bytes. Hence, TCP groups a number of bytes together into a *segment* and adds a header to each of these segments and then delivers these segments to the network layer. At the network layer, each of these segments is encapsulated in an IP packet for transmission. The TCP header has information that is required for control purposes which will be discussed along with the segment structure.

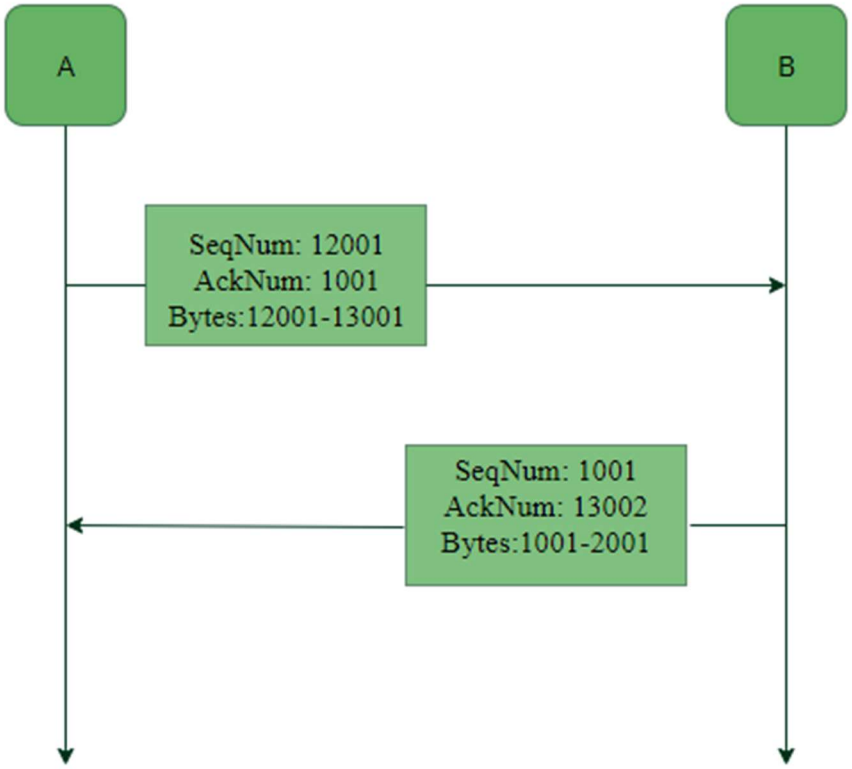
3. **Full-duplex service –**
   This means that the communication can take place in both directions at the same time.

4. **Connection-oriented service –**
   Unlike UDP, TCP provides a connection-oriented service. It defines 3 different phases:
   - Connection establishment
   - Data transfer
   - Connection termination
5. **Reliability –**
   TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgement policy and timers. It uses features like byte number and sequence number and acknowledgement number so as to ensure reliability. Also, it uses congestion control mechanisms.

6. **Multiplexing –**
   TCP does multiplexing and de-multiplexing at the sender and receiver ends respectively as a number of logical connections can be established between port numbers over a physical connection.

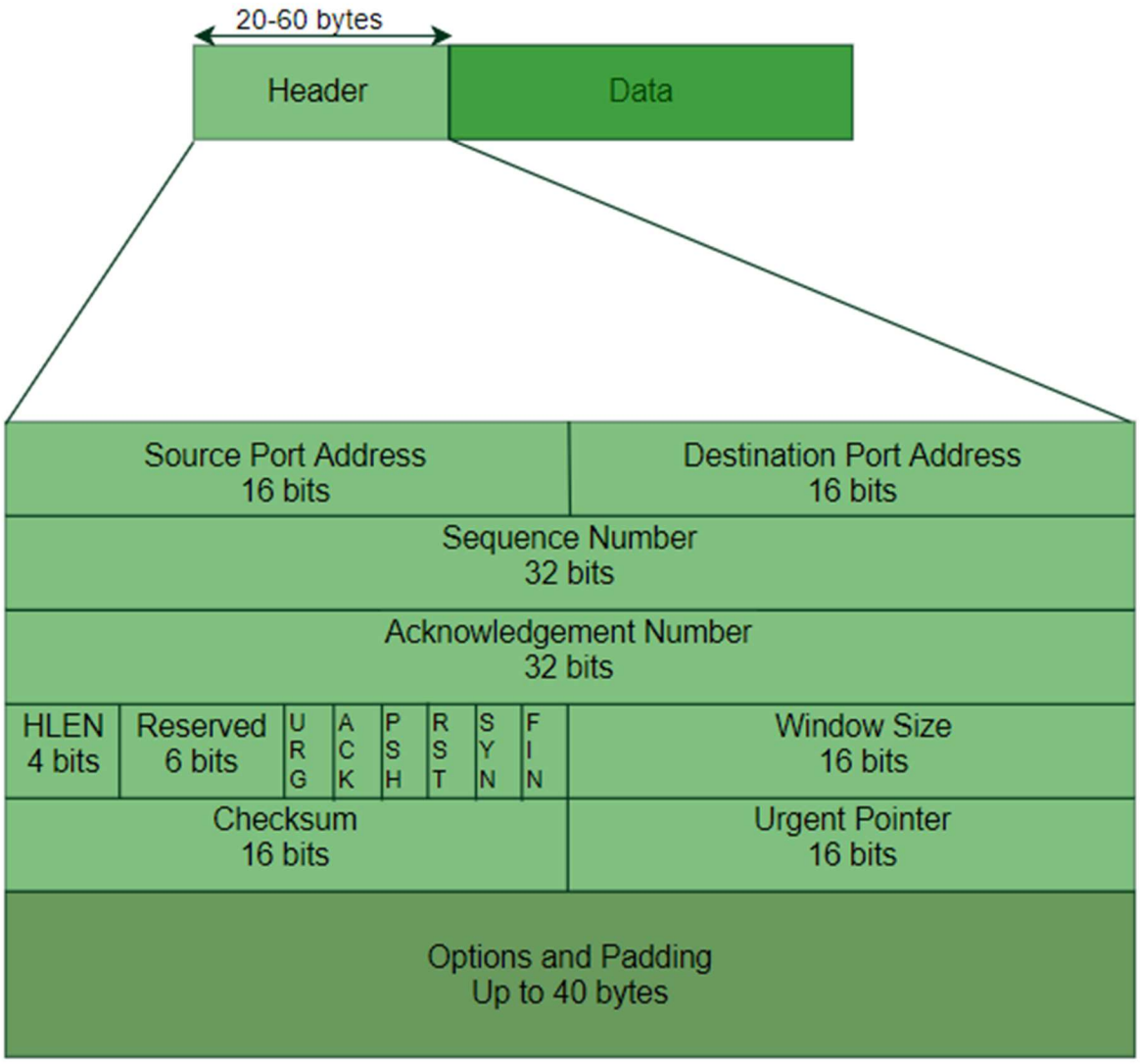
Byte number, Sequence number and Acknowledgement number:
All the data bytes that are to be transmitted are numbered and the beginning of this numbering is arbitrary. Sequence numbers are given to the segments so as to reassemble the bytes at the receiver end even if they arrive in a different order. The sequence number of a segment is the byte number of the first byte that is being sent. The acknowledgement number is required since TCP provides full-duplex service. The acknowledgement number is the next byte number that the receiver expects to receive which also provides

acknowledgement for receiving the previous bytes.
Example:



In this example we see that A sends acknowledgement number1001, which means that it has received data bytes till byte number 1000 and expects to receive 1001 next, hence B next sends data bytes starting from 1001. Similarly, since B has received data bytes till byte number 13001 after the first data transfer from A to B, therefore B sends acknowledgement number 13002, the byte number that it expects to receive from A next.

TCP Segment structure –
A TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown:



The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes.
Header fields:

- **Source Port Address –**
  A 16-bit field that holds the port address of the application that is sending the data segment.

- **Destination Port Address –**
  A 16-bit field that holds the port address of the application in the host that is receiving the data segment.

- **Sequence Number –**
  A 32-bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.

- **Acknowledgement Number –**
  A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

- **Header Length (HLEN) –**
  This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

- **Control flags –**
  These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:
    - URG: Urgent pointer is valid
    - ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)
    - PSH: Request for push
    - RST: Reset the connection
    - SYN: Synchronize sequence numbers
    - FIN: Terminate the connection
- **Window size –**
  This field tells the window size of the sending TCP in bytes.

- **Checksum –**
  This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

- **Urgent pointer –**
  This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get

the byte number of the last urgent byte.

TCP Connection –
TCP is connection-oriented. A TCP connection is established by a 3-way handshake.

FLOW CONTROL AND CONGESION CONTROL :

Flow Control and **Congestion Control** are traffic controlling methods for different situations. The main difference between flow control and congestion control is that, In flow control, rate of traffic received from a sender can be controlled by a receiver. On the other hand, In congestion control, rate of traffic from sender to the network is controlled.

Flow Control:

Flow control is a technique used to regulate the flow of data between different nodes in a network. It ensures that a sender does not overwhelm a receiver with too much data too quickly. The goal of flow control is to prevent buffer overflow, which can lead to dropped packets and poor network performance.

Advantages of Flow Control:

- Prevents buffer overflow: Flow control prevents buffer overflow by regulating the rate at which data is sent from the sender to the receiver.
- Helps in handling different data rates: Flow control helps in handling different data rates by regulating the flow of data to match the capacity of the receiving device.
- Efficient use of network resources: Flow control helps in efficient use of network resources by avoiding packet loss and reducing the need for retransmissions.

Disadvantages of Flow Control:

- May cause delays: Flow control may cause delays in data transmission as it regulates the rate of data flow.
- May not be effective in congested networks: Flow control may not be effective in congested networks where the congestion is caused by multiple sources.
- May require additional hardware or software: Flow control may require additional hardware or software to implement the flow control mechanism.

Congestion Control:

Congestion control is a technique used to prevent congestion in a network. Congestion occurs when too much data is being sent over a network, and the network becomes overloaded, leading to dropped packets and poor network performance.

Advantages of Congestion Control:

- Prevents network congestion: Congestion control prevents network congestion by regulating the rate at which data is sent from the sender to the receiver.
- Efficient use of network resources: Congestion control helps in efficient use of network resources by reducing the number of lost packets and retransmissions.
- Fair allocation of network resources: Congestion control ensures a fair allocation of network resources by regulating the rate of data flow for all sources.
-

Disadvantages of Congestion Control:

- May cause delays: Congestion control may cause delays in data transmission as it regulates the rate of data flow.
- May require additional hardware or software: Congestion control may require additional hardware or software to implement the congestion control mechanism.
- May lead to underutilization of network resources: Congestion control may lead to underutilization of network resources if the congestion is not severe.

Similarities between Flow Control and Congestion Control:

- Both regulate the flow of data: Both flow control and congestion control regulate the flow of data in a network.
- Both prevent packet loss: Both flow control and congestion control prevent packet loss by regulating the rate of data flow.

Both improve network efficiency: Both flow control and congestion control improve network efficiency by reducing the number of lost packets and retransmissions.

difference between flow control and congestion control:

S.NO	Flow Control	Congestion Control
1.	Traffic from sender to receiver is controlled, to avoid overwhelming the slow receiver.	Traffic entering the network from a sender is controlled by reducing rate of packets. Here, the sender has to control/modulate his own rate to achieve optimal network utilization.
2.	Flow control is typically used in data link layer.	Congestion control is applied in network and transport layer.
3.	In this, Receiver's data is prevented from being overwhelmed.	In this, Network is prevented from congestion.
4.	In flow control, sender needs to take measures to avoid receiver from being overwhelmed depending on feedback from receiver and also in absence of any feedback.	In this, many algorithms designed for transport layer/network layer define how endpoints should behave to avoid congestion.
5.	Types of Flow control are 1. Stop and Wait – For every frame transmitted, sender expects ACK from receiver. 2. Sliding Window – ACK needed only after sender transmits data until window is full, which is allocated initially by receiver.	Mechanisms designed to prevent network congestions are 1. Network Queue Management 2. Explicit Congestion Notification 3. TCP Congestion control

Network Layer :

he network Layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination. It involves both the source host and the destination host.
Key among these services are packetizing, routing, and forwarding. Packetizing involves encapsulating data into packets suitable for transmission. Routing determines the optimal path for these packets through the network, ensuring they navigate through multiple nodes and networks efficiently. Forwarding is the process of directing these packets to their next hop along the selected path.

Features of Network Layer

- The main responsibility of the Network layer is to carry the data packets from the source to the destination without changing or using them.
- If the packets are too large for delivery, they are fragmented i.e., broken down into smaller packets.
- It decides the route to be taken by the packets to travel from the source to the destination among the multiple routes available in a network (also called routing).
- The source and destination addresses are added to the data packets inside the network layer.

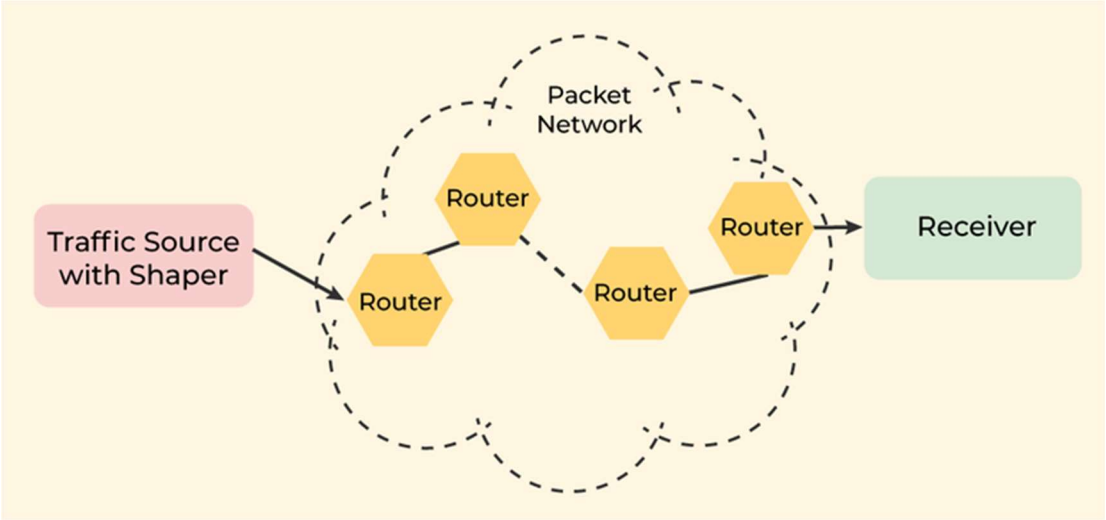
Services Offered by Network Layer

The **services** which are offered by the network layer protocol are as follows:

1. Packetizing

The process of encapsulating the data received from the upper layers of the network (also called payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.
The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol and delivers the packet to the data link layer.

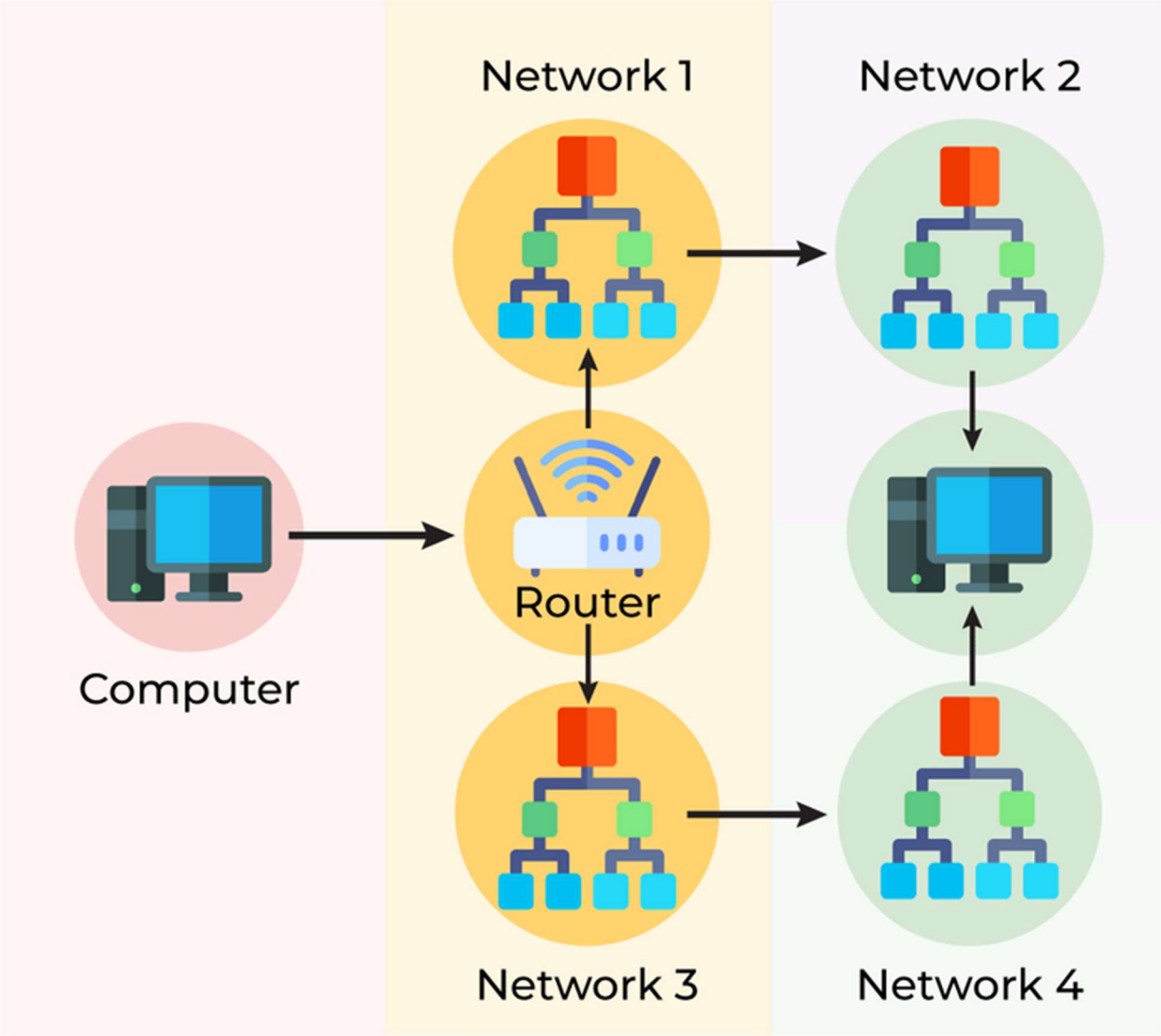
The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol. The routers in the path are not allowed to change either the source or the destination address. The routers in the path are not allowed to decapsulate the packets they receive unless they need to be fragmented.



Packetizing

2. Routing

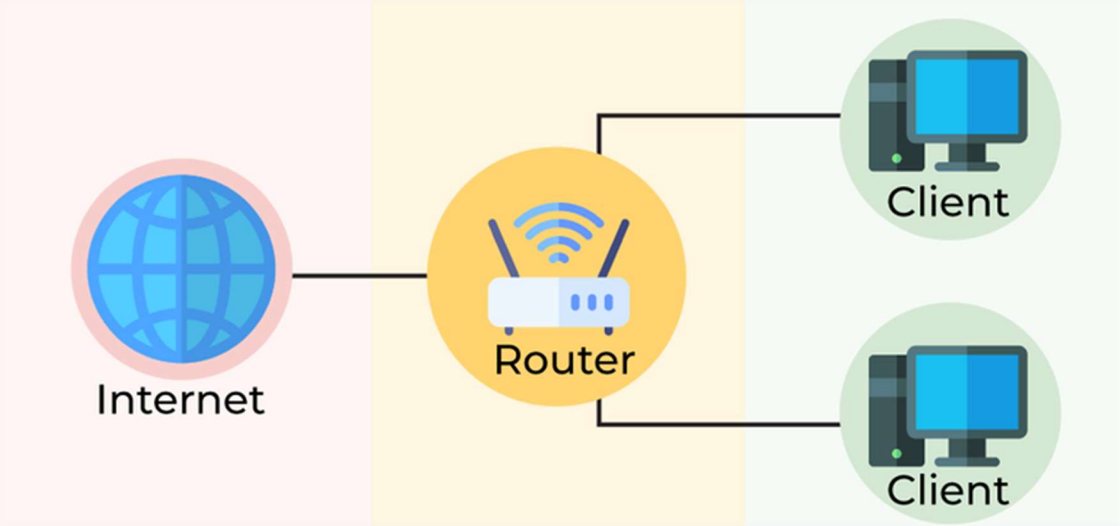
Routing is the process of moving data from one device to another device. These are two other services offered by the network layer. In a network, there are a number of routes available from the source to the destination. The network layer specifies some strategies which find out the best possible route. This process is referred to as routing. There are a number of routing protocols that are used in this process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.



Routing

3. Forwarding

Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks (in the case of multicast routing). Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves packet forwarding from an entry interface out to an exit interface.



Forwarding

Differences Between Routing and Forwarding

Routing	Forwarding
Routing is the process of moving data from one device to another device.	Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces.
Operates on the Network Layer.	Operates on the Network Layer.
Work is based on Forwarding Table.	Checks the forwarding table and work according to that.
Works on protocols like Routing Information Protocol (RIP) for Routing.	Works on protocols like UDP Encapsulating Security Payloads

Other Services Expected from Network Layer

- Error Control
- Flow Control
- Congestion Control

1. Error Control

Although it can be implemented in the network layer, it is usually not preferred because the data packet in a network layer may be fragmented at each router, which makes error-checking inefficient in the network layer.

2. Flow Control

It regulates the amount of data a source can send without overloading the receiver. If the source produces data at a very faster rate than the receiver can consume it, the receiver will be overloaded with data. To control the flow of data, the receiver should send feedback to the sender to inform the latter that it is overloaded with data.
There is a lack of flow control in the design of the network layer. It does not directly provide any flow control. The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

3. Congestion Control

Congestion occurs when the number of datagrams sent by the source is beyond the capacity of the network or routers. This is another issue in the network layer protocol. If congestion continues, sometimes a situation may arrive where the system collapses and no datagrams are delivered. Although congestion control is indirectly implemented in the network layer, still there is a lack of congestion control in the network layer.

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.

Differences Between Virtual Circuits and Datagram Networks

Virtual Circuits

- It is connection-oriented, meaning that there is a reservation of resources like buffers, CPU, bandwidth, etc. for the time in which the newly set VC is going to be used by a data transfer session.
- The first sent packet reserves resources at each server along the path. Subsequent packets will follow the same path as the first sent packet for the connection time.
- Since all the packets are going to follow the same path, a global header is required. Only the first packet of the connection requires a global header, the remaining packets generally don't require global headers.
- Since all packets follow a specific path, packets are received in order at the destination.
- Virtual Circuit Switching ensures that all packets successfully reach the Destination. No packet will be discarded due to the unavailability of resources.
- From the above points, it can be concluded that Virtual Circuits are a highly reliable method of data transfer.
- The issue with virtual circuits is that each time a new connection is set up, resources and extra information have to be reserved at every router along the path, which becomes problematic if many clients are trying to reserve a router's resources simultaneously.
- It is used by the ATM (Asynchronous Transfer Mode) Network, specifically for Telephone calls.

Types of Virtual Circuit

1. Permanent Virtual Circuits(PVC): The communication management station, which is the telco's central office, manually configures the switches, which offer performance comparable to dedicated lines. The main use for these always-on circuits is high-speed communication. PVCs require telco resources (switches) to be allocated to a single communication circuit whether or not that circuit is in use, making them an expensive solution for wide-area networks (WANs).
2. Switched Virtual circuits (SVCs): As soon as a communication session is established, the switches are set up. SVCs are released at the conclusion of the session and can be used to create new channels of communication. This

is the process of normal phone communication. SVCs, which are billed on a per-minute basis, are generally utilized in WANs when backups to dedicated leased lines are required.

Benefits of Virtual Circuit

- The recipient receives the sender's packets in the same order as they were sent.
- A secure network link is called a virtual circuit.
- Overhead is not required for any packet.
- A single global packet overhead is used in a virtual circuit.

Drawbacks of Virtual Circuits

- The cost of implementing a virtual circuit is high.
- It provides only services based on connections.
- In order to transmit, a new link needs to be created permanently.
-

Datagram Networks

- It is a connection-less service. There is no need for reservation of resources as there is no dedicated path for a connection session.
- All packets are free to use any available path. As a result, intermediate routers calculate routes on the go due to dynamically changing routing tables on routers.
- Since every packet is free to choose any path, all packets must be associated with a header with proper information about the source and the upper layer data.
- The connection-less property makes data packets reach the destination in any order, which means that they can potentially be received out of order at the receiver's end.
- Datagram networks are not as reliable as Virtual Circuits.
- The major drawback of Datagram Packet switching is that a packet can only be forwarded if resources such as the buffer, CPU, and bandwidth are available. Otherwise, the packet will be discarded.
- But it is always easy and cost-efficient to implement datagram networks as there is no extra headache of reserving resources and making a dedicated each time an application has to communicate.
- It is generally used by the IP network, which is used for Data services like the Internet.

Benefits of Datagram Networks

- The flexibility of datagram networks is one of its main benefits.

- They are better at managing network congestion. Datagram networks are able to adjust to variations in network traffic and identify several paths for packets to take in order to reach their intended destination because every packet is handled separately.
- In big and complicated networks in particular, this can lead to decreased latency and increased network performance.
- In addition, datagram networks scale more easily than other kinds of networks. Datagram networks are the ideal option for contemporary communication systems, such as the Internet of Things (IoT) and real-time data streaming applications, due to their scalability.
-

Drawbacks of Datagram Networks

- The lack of assured delivery in datagram networks is one of their primary disadvantages. There is no assurance that all packets will arrive at their destination or in the right order because they are sent separately.
- Datagram networks also have the drawback of being vulnerable to security breaches. Datagram networks are particularly susceptible to network assaults including spoofing, eavesdropping, and denial of service (DoS) attacks since they don't create a dedicated connection between the sender and the recipient.
- Moreover, datagram networks may not always support guarantees of quality of service (QoS). While certain applications may benefit from QoS capabilities provided by some protocols, like the Real-time Transport Protocol (RTP), datagram networks as a whole do not provide a centralised method for allocating priorities and controlling network traffic.

Difference Between Virtual Circuits and Datagram Networks

Criteria	Virtual Circuit Networks	Datagram Networks
Connection Establishment	Prior to data transmission, a connection is established between sender and receiver.	No connection setup is required.

Criteria	Virtual Circuit Networks	Datagram Networks
Routing	Routing decisions are made once during connection setup and remain fixed throughout the duration of the connection.	Routing decisions are made independently for each packet and can vary based on network conditions.
Flow Control	Uses explicit flow control, where the sender adjusts its rate of transmission based on feedback from the receiver.	Uses implicit flow control, where the sender assumes a certain level of available bandwidth and sends packets accordingly.
Congestion Control	Uses end-to-end congestion control, where the sender adjusts its rate of transmission based on feedback from the network.	Uses network-assisted congestion control, where routers monitor network conditions and may drop packets or send congestion signals to the sender.
Error Control	Provides reliable delivery of packets by detecting and retransmitting lost or corrupted packets.	Provides unreliable delivery of packets and does not guarantee delivery or correctness.
Overhead	Requires less overhead per packet because connection setup and state maintenance are done only once.	Requires more overhead per packet because each packet contains information about its

Criteria	Virtual Circuit Networks	Datagram Networks
		destination address and other routing information.
Example Protocol	ATM, Frame Relay	IP (Internet Protocol)

The internals of a router:

A Router is a networking device that fulfills the need for devices to share files and forward data packets between devices over computer networks. Routers perform some directing functions on the Internet so the data sent over the internet, such as a web page in the form of data packets

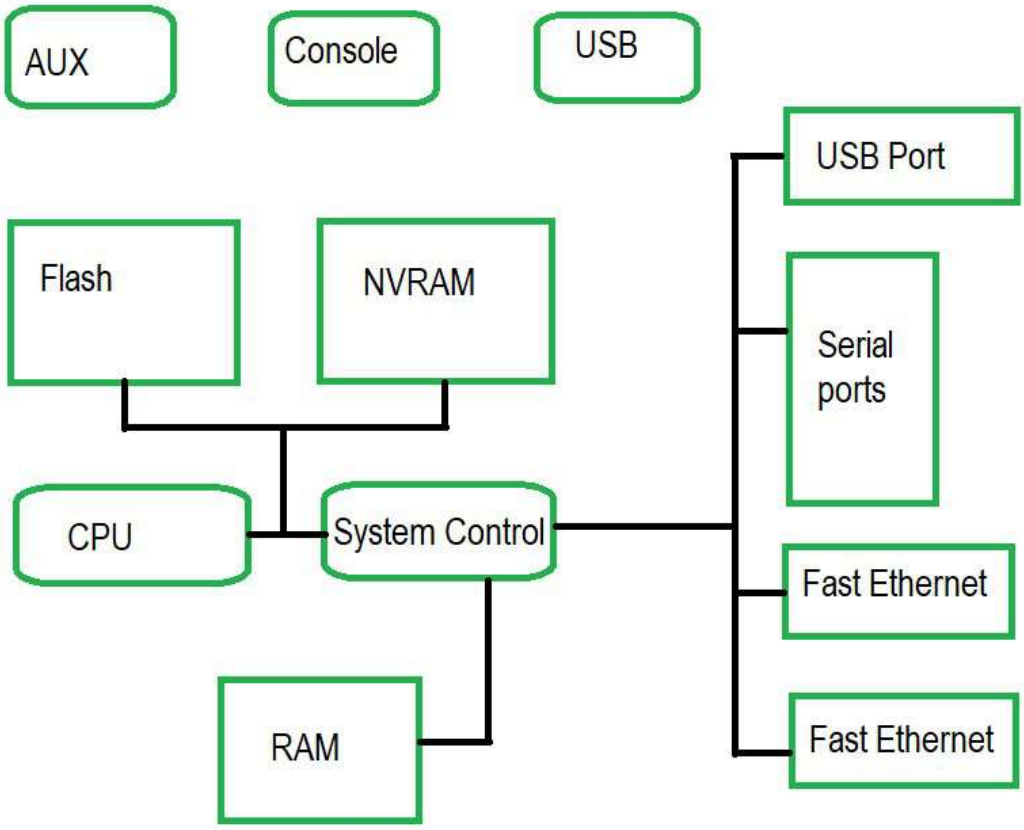
A wireless router connects directly to a modem by a cable then a router can receive and transmit information or data to the internet. Then the router starts to communicate with the wifi network and provides internet access to all devices within the network range of the router.

A generic router consists of the following components:

1. **Input Port:** This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at the router
2. **Switching Fabric:** This is the main component of the Router, it connects the input ports with the output ports. It is kind of a network inside a networking device.
3. **Output Ports:** This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets
4. **Routing Processor:** It executes the routing protocols, and works like a traditional CPU. It uses various routing algorithms like link-state algorithm, distance-vector algorithm, etc.

The Internal Components of Router:

Below is the raw diagram showing the internal components of the router:



Internal Components of Router

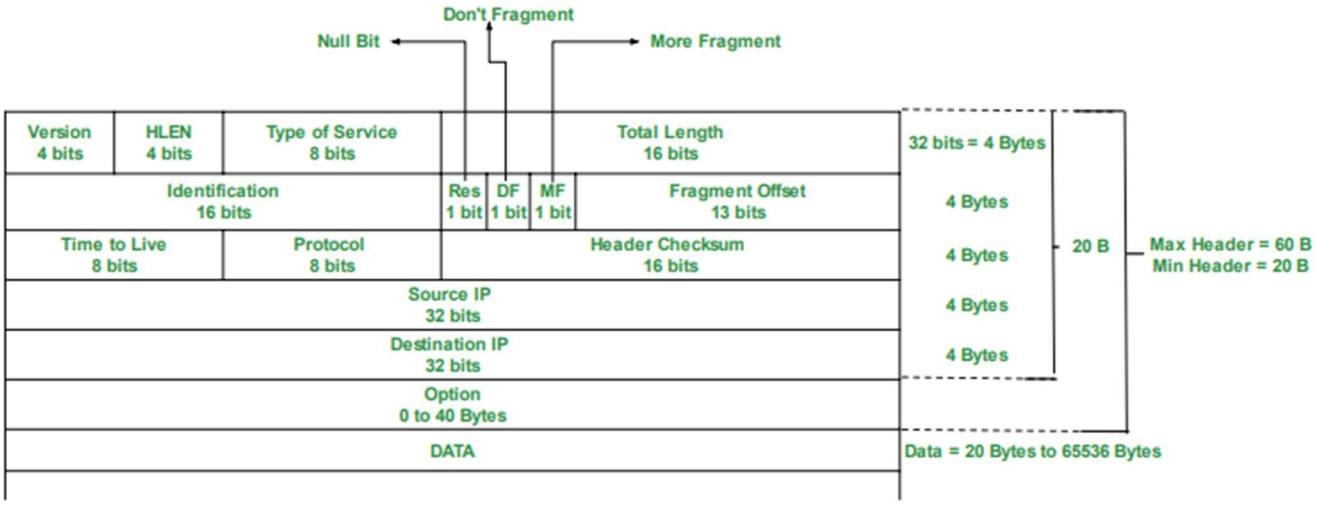
The router is an intelligent device, routers use routing algorithms such as **Dijkstra's Algorithm** to map the destination or to find the best route to a destination on the parameters like the number of hops.

1. **CPU:** The CPU in the router executes the commands and processes the commands in the operating system. The flow of data on the interface is controlled by the CPU.

2. **ROM:** Read Only Memory in the router mainly works when the router boots up or is powered up. It stores the bootstrap program needed when the router is turned on.
3. **RAM:** Random Access Memory in the router contains the executable file and running file of the configuration file and the contents are lost when the router's power is turned off.
4. **Flash Memory:** It contains the operating system. The data of the flash memory remain unchanged when the router is rebooted or powered off. So, whenever the router is powered on the OS is loaded into RAM from flash memory.
5. **NVRAM:** It stands for Nonvolatile RAM. It is a backup copy of the running configuration file. Its functioning basically helps when the router loses power and the router needs to establish the configuration and load it again. The content of NVRAM is changeable. When the router is powered on it searches the startup-config file in NVRAM only.
6. **Interfaces / Ports:** If we want to connect the router with wire or we want a wired connection there are multiple interfaces that are used to connect the network. i.e. Fast Ethernet, Gigabit Ethernet, and Serial.

The Internet Protocol(IP), Datagram format:

IPv4 Datagram Header Size of the header is 20 to 60 bytes.



IPv4 Datagram Header

VERSION: *Version of the IP protocol (4 bits), which is 4 for IPv4*
HLEN: *IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*

Type of service: *Low Delay, High Throughput, Reliability (8 bits)*
Total Length: *Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*
Identification: *Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*
Flags: *3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*
Fragment Offset: *Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*
Time to live: *Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*
Protocol: *Name of the protocol to which the data is to be passed (8 bits)*
Header Checksum: *16 bits header checksum for checking errors in the datagram header*
Source IP address: *32 bits IP address of the sender*
Destination IP address: *32 bits IP address of the receiver*
Option: *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

IP 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.

- 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.

the 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.

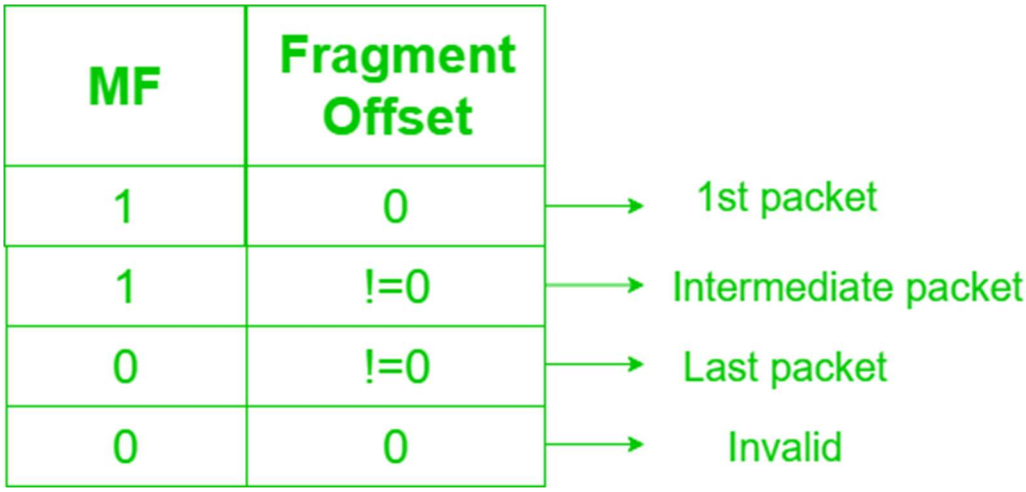
Fragmentation at the network layer allows the packet to be divided into smaller fragments that can be transmitted over networks with different MTU values.
3.Reliable Transmission: Fragmentation at the network layer increases the reliability of data transmission, as smaller fragments are less likely to be lost or corrupted during transmission.

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 $\in$ 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.



Algorithm –

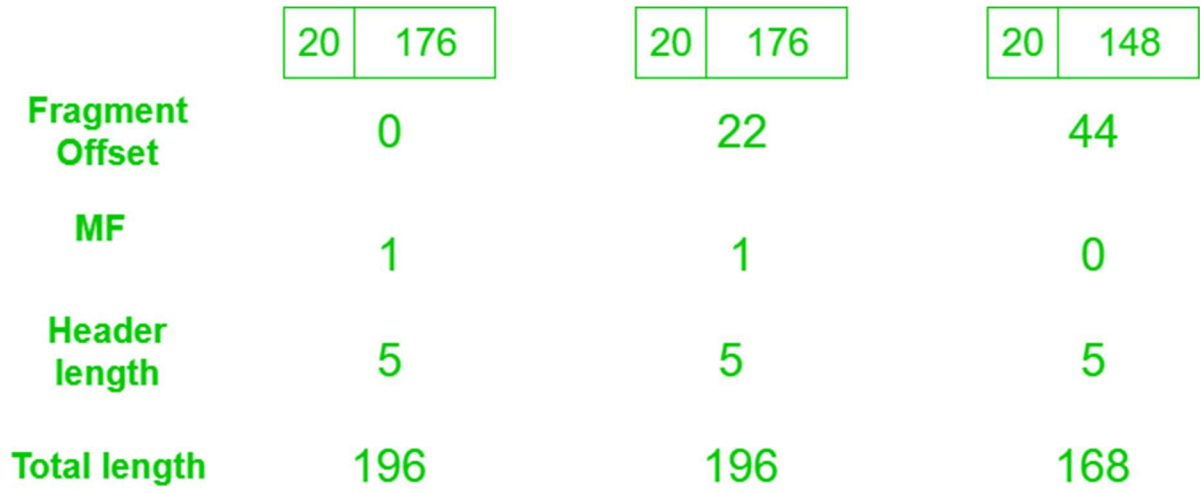
1. Destination should identify that datagram is fragmented from MF, Fragment offset field.
2. Destination should identify all fragments belonging to same datagram from Identification field.
3. Identify the 1st fragment(offset = 0).
4. Identify subsequent fragments using header length, fragment offset.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



IPV4 addressing:

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

Parts of IPv4

- **Network part:**
  The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:**
  The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.

- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

Advantages of IPv4

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

Limitations of IPv4

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

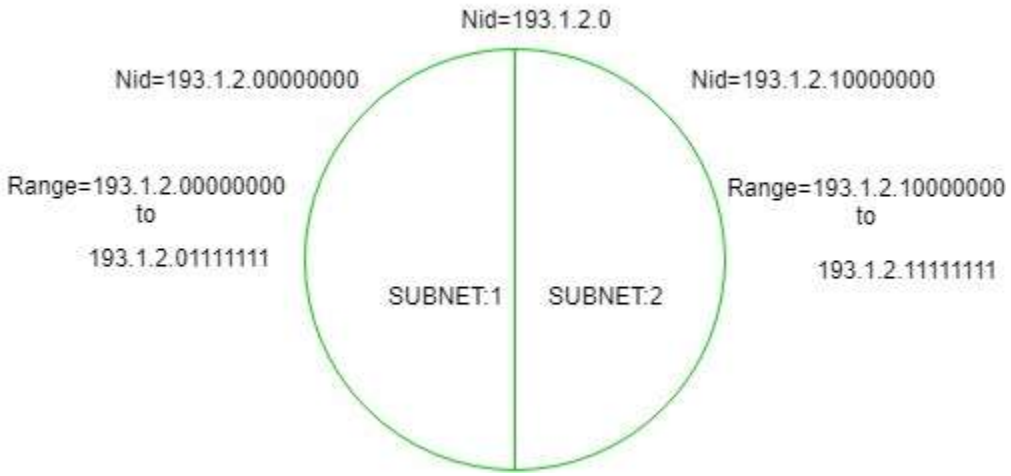
Subnets:

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

Uses of Subnetting

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

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



In the above diagram, there are two Subnets.

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

How Does Subnetting Work?

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

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

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

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

```
Subnet id of Subnet-1 is : 193.1.2.0
The direct Broadcast id of Subnet-1 is: 193.1.2.127
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 1 is: 255.255.255.128
```

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

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

```
Subnet id of Subnet-2 is : 193.1.2.128
The direct Broadcast id of Subnet-2 is: 193.1.2.255
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id &  Direct Broadcast id)
The subnet mask of Subnet- 2 is: 255.255.255.128
The best way to find out the subnet mask of a subnet
is to set the fixed bit of host-id to 1 and the rest to 0.
```

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

Note:

1. To divide a network into four (2_2) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2_3) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

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

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

1. 201.35.2.129
2. 201.35.2.191

3. 201.35.2.255
4. Both (A) and (C)

Solution:

```
Converting the last octet of the
netmask into the binary form: 255.255.255.11000000
Converting the last octet of option 1
 into the binary form: 201.35.2.10000001
Converting the last octet of option 2
into the binary form: 201.35.2.10111111
Converting the last octet of option 3
into the binary form: 201.35.2.11111111
```

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

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

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

Solution:

```
Converting the last octet of the netmask
 into the binary form: 255.255.255.11111000
Converting the last octet of option 1
into the binary form: 201.32.64.10000111
Converting the last octet of option 2
into the binary form: 201.32.64.11110000
Converting the last octet of option 3
into the binary form: 201.32.64.11001111
Converting the last octet of option 4
into the binary form: 201.32.64.11100111
```

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

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

Advantages of Subnetting

The advantages of Subnetting are mentioned below:

1. It provides security to one network from another network. eg) In an Organisation, the code of the Developer department must not be accessed by another department.

2. It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department needs to host webcasts or video conferences.
3. In the case of Small networks, maintenance is easy.

Disadvantages of Subnetting

The disadvantages of Subnetting are mentioned below:

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

CIDR:

Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.

CIDR addresses are represented using a slash notation, which specifies the number of bits in the network prefix. For example, an IP address of 192.168.1.0 with a prefix length of 24 would be represented as 192.168.1.0/24. This notation indicates that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier.

Several Advantages of the Traditional Class-Based Addressing System of CIDR

- Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses by allowing the allocation of IP addresses based on their network prefix rather than their class.
- Flexibility: CIDR allows for more flexible IP address allocation, as it allows for the allocation of arbitrary-sized blocks of IP addresses.
  Better routing: CIDR allows for better routing of IP traffic, as it allows

routers to aggregate IP addresses based on their network prefix, reducing the size of routing tables.
- Reduced administrative overhead: CIDR reduces administrative overhead by allowing for the allocation and routing of IP addresses in a more efficient and flexible way.
- In summary, CIDR is a method of IP address allocation and routing that allows for more efficient use of IP addresses and better routing of IP traffic. It has several advantages over the traditional class-based addressing system, including greater flexibility, better routing, and reduced administrative overhead.

As with any technology or system, there are advantages and disadvantages of using CIDR:

Advantages of CIDR

- Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses, which is important as the pool of available IPv4 addresses continues to shrink.
- Flexibility: CIDR allows for more flexible allocation of IP addresses, which can be important for organizations with complex network requirements.
- Better routing: CIDR allows for more efficient routing of IP traffic, which can lead to better network performance. Reduced administrative overhead: CIDR reduces administrative overhead by allowing for easier management of IP addresses and routing.

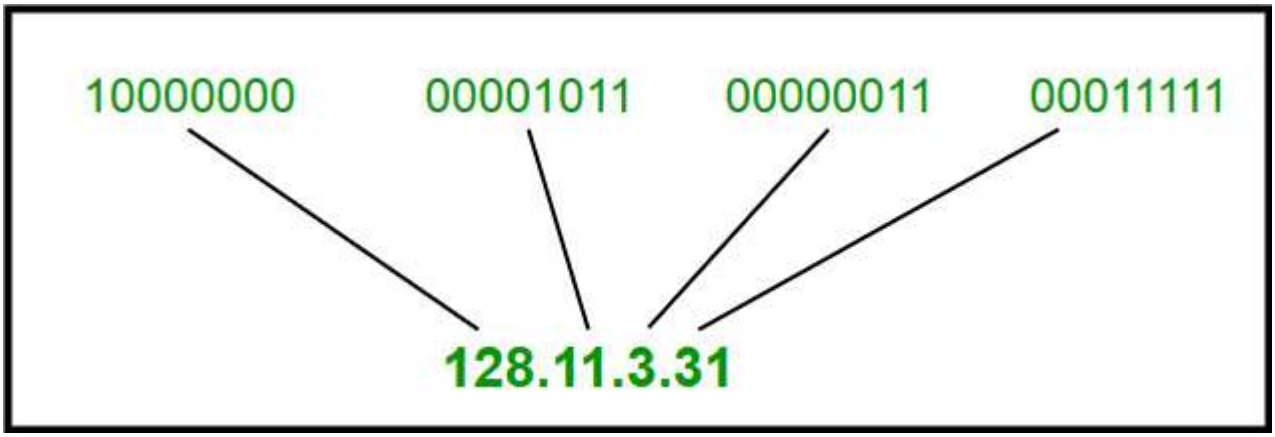
Disadvantages of CIDR

- Complexity: CIDR can be more complex to implement and manage than traditional class-based addressing, which can require additional training and expertise.
- Compatibility issues: Some older network devices may not be compatible with CIDR, which can make it difficult to transition to a CIDR-based network.
- Security concerns: CIDR can make it more difficult to implement security measures such as firewall rules and access control lists, which can increase security risks.
- Overall, CIDR is a useful and efficient method of IP address allocation and routing, but it may not be suitable for all organizations or networks. It is important to weigh the advantages and disadvantages of CIDR and consider the specific needs and requirements of your network before implementing CIDR.

classful addressing:

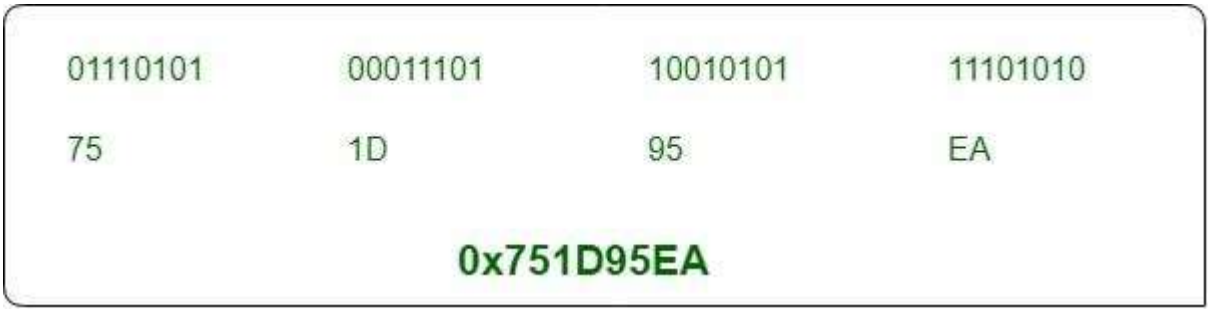
An IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32-bit unique address having an address space of 2^{32}. Generally, there are two notations in which the IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation



Dotted Decimal Notation

Hexadecimal Notation



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).

Classful Addressing

The 32-bit IP address is divided into five sub-classes. These are given below:

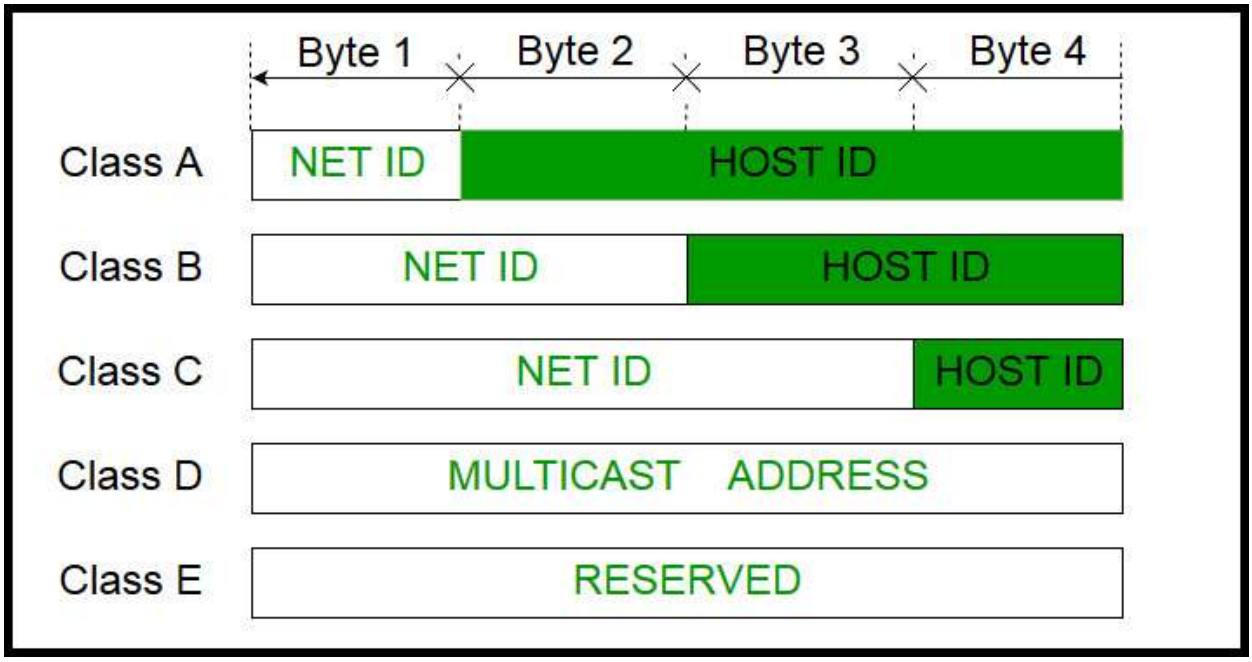
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of

bits in the first octet determines the classes of the IP address. The IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.



1. IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).
2. While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits

of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 0.0.0.0 – 127.255.255.255.

Class A

Class B

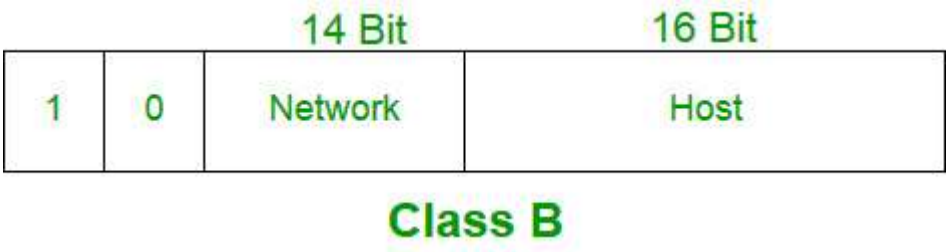
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.



Class B

Class C

IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits

of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

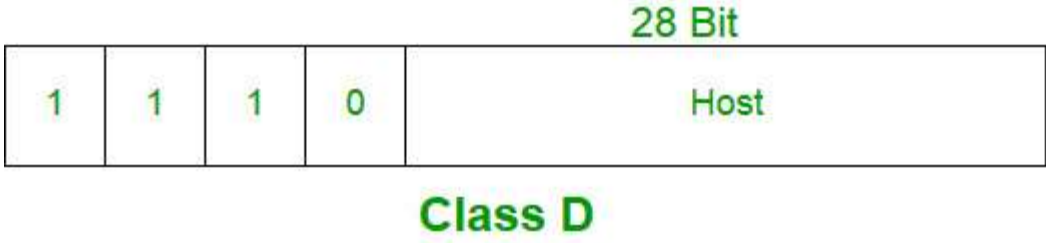
IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

Class C

Class D

IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

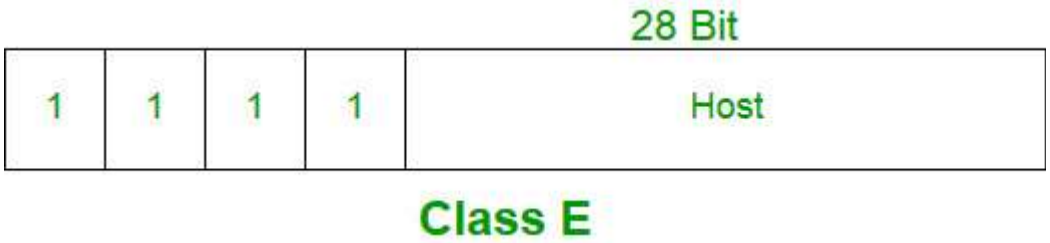
Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



Class D

Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Class E

Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.255.255.255 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful Addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

In the above table No. of networks for class A should be 127. (Network ID with all 0 s is not considered)

Problems with Classful Addressing

The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in the next post.

- The network ID is 24 bits long.
- The host ID is 8 bits long.
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address
- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.
- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren’t used.

DHCP:

Dynamic Host Configuration Protocol, is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network.

What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients’ devices such as desktops, laptops, cellphones, etc. is an application layer protocol that is used to provide:

```
Subnet Mask (Option 1 - e.g., 255.255.255.0)
Router Address (Option 3 - e.g., 192.168.1.1)
DNS Address (Option 6 - e.g., 8.8.8.8)
Vendor Class Identifier (Option 43 - e.g.,
'unifi' = 192.168.1.9 ##where unifi = controller)
```

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

Why Use DHCP?

DHCP helps in managing the entire process automatically and centrally. DHCP helps in maintaining a unique IP Address for a host using the server. DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer

Components of DHCP

The main components of DHCP include:

- **DHCP Server:** DHCP Server is a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.
- **DNS Servers:** DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- **Default Gateway:** DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- **Options:** DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name, and time server information.

- **Renewal:** DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.
- **Failover:** DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- **Dynamic Updates:** DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- **Audit Logging:** DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

Operation Code	Hardware type	Hardware length	Hop count
Transition ID			
Number of seconds		Flags	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot file name (128 bytes)			

Operation Code	Hardware type	Hardware length	Hop count
Options (Variable length)			

Fig. DHCP Packet

Format

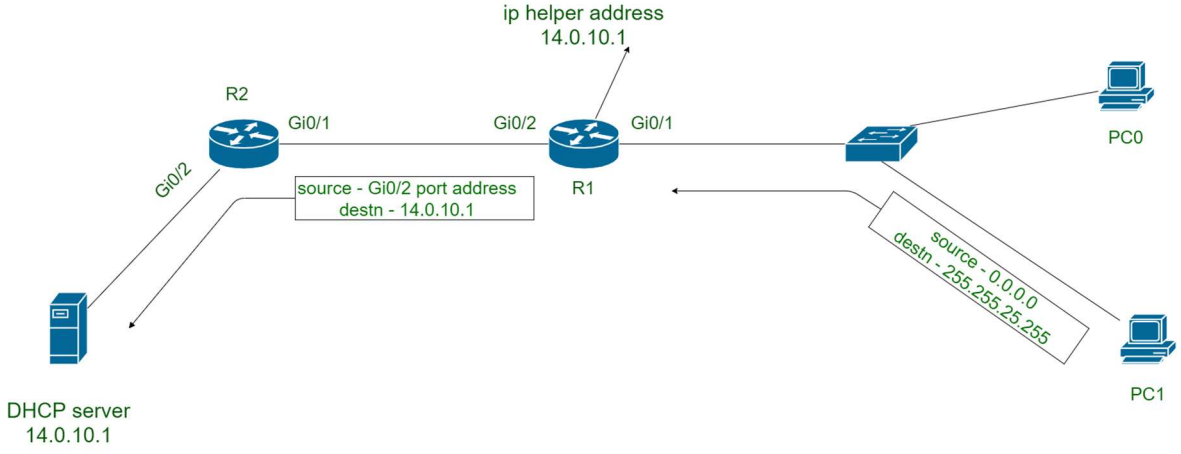
- **Hardware length:** This is an 8-bit field defining the length of the physical address in bytes. e.g for Ethernet the value is 6.
- **Hop count:** This is an 8-bit field defining the maximum number of hops the packet can travel.
- **Transaction ID:** This is a 4-byte field carrying an integer. The transcation identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.
- **Number of seconds:** This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.
- **Flag:** This is a 16-bit field in which only the leftmost bit is used and the rest of the bit should be set to os. A leftmost bit specifies a forced broadcast reply from the server. If the reply were to be unicast to the client, the destination. IP address of the IP packet is the address assigned to the client.
- **Client IP address:** This is a 4-byte field that contains the client IP address . If the client does not have this information this field has a value of 0.
- **Your IP address:** This is a 4-byte field that contains the client IP address. It is filled by the server at the request of the client.
- **Server IP address:** This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.
- **Gateway IP address:** This is a 4-byte field containing the IP address of a routers. IT is filled by the server in a reply message.
- **Client hardware address:** This is the physical address of the client .Although the server can retrieve this address from the frame sent by the client it is more efficient if the address is supplied explicity by the client in the request message.
- **Server name:** This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this filed with data, the server must fill it with all 0s.

- **Boot filename:** This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null- terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.
- **Options:** This is a 64-byte field with a dual purpose. IT can carry either additional information or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present the next 60 bytes are options.

Working of DHCP

DHCP works on the Application layer of the TCP/IP Protocol. The main task of DHCP is to dynamically assigns IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients. For more, you can refer to the Article Working of DHCP.

The DHCP **port number** for the server is 67 and for the client is 68. It is a client-server protocol that uses UDP services. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the DORA process, but there are 8 DHCP messages in the process.

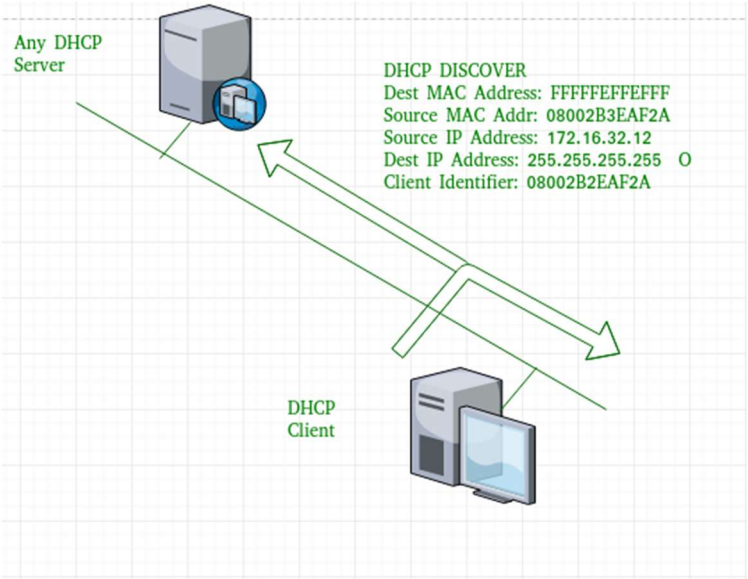


Working of DHCP

The 8 DHCP Messages

1. DHCP discover message: This is the first message generated in the communication process between the server and the client. This message is generated by the Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted

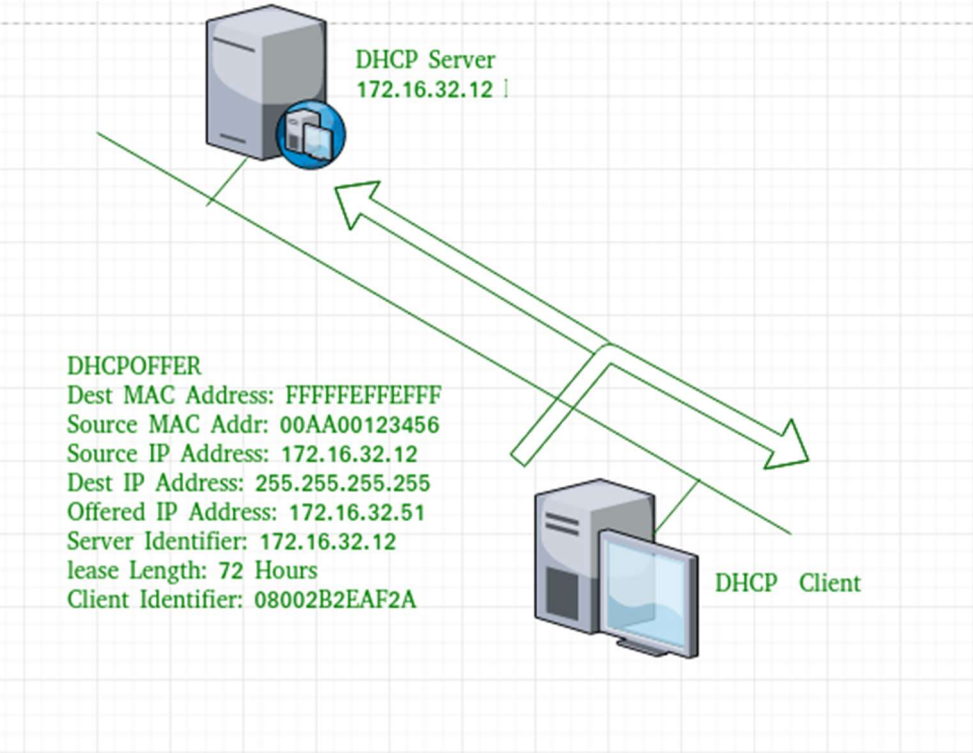
to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



DHCP discover message

As shown in the figure, the source MAC address (client PC) is 08002B2EAF2A, the destination MAC address(server) is FFFFFFFFFFFF, the source IP address is 0.0.0.0(because the PC has had no IP address till now) and the destination IP address is 255.255.255.255 (IP address used for broadcasting). As they discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

2. DHCP offers a message: The server will respond to the host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by the server. The size of the message is 342 bytes. If there is more than one DHCP server present in the network then the client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.

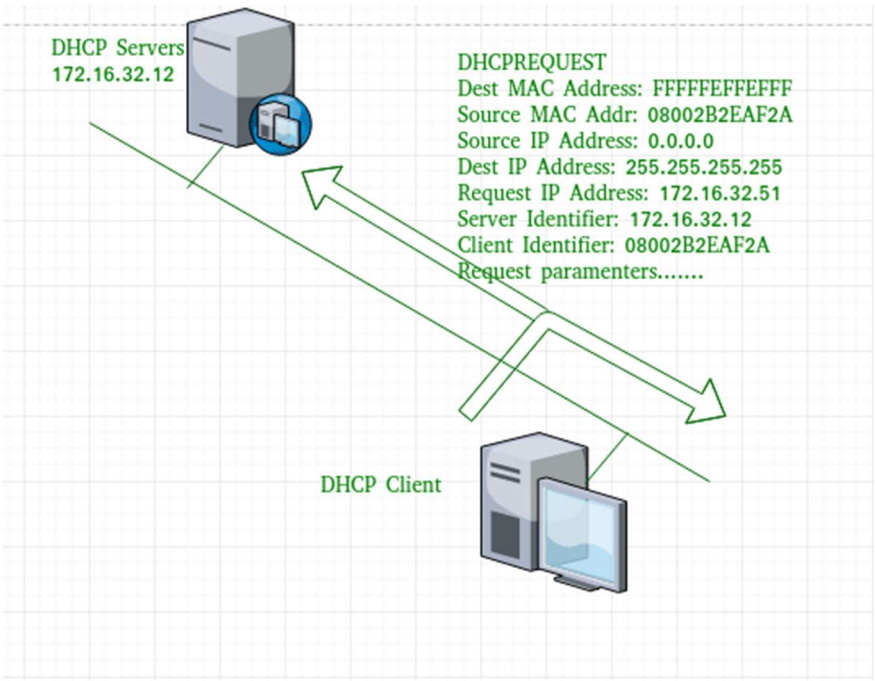


DHCP offer message

Now, for the offer message, the source IP address is 172.16.32.12 (server's IP address in the example), the destination IP address is 255.255.255.255 (broadcast IP address), the source MAC address is 00AA00123456, the destination MAC address is FFFFFFFFFFFF. Here, the offer message is broadcast by the DHCP server therefore destination IP address is the broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is the server IP address and the MAC address is the server MAC address.

Also, the server has provided the offered IP address 192.16.32.51 and a lease time of 72 hours(after this time the entry of the host will be erased from the server automatically). Also, the client identifier is the PC MAC address (08002B2EAF2A) for all the messages.

3. DHCP request message: When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with the same IP address. If there is no reply from another host, then there is no host with the same TCP configuration in the network and the message is broadcasted to the server showing the acceptance of the IP address. A Client ID is also added to this message.

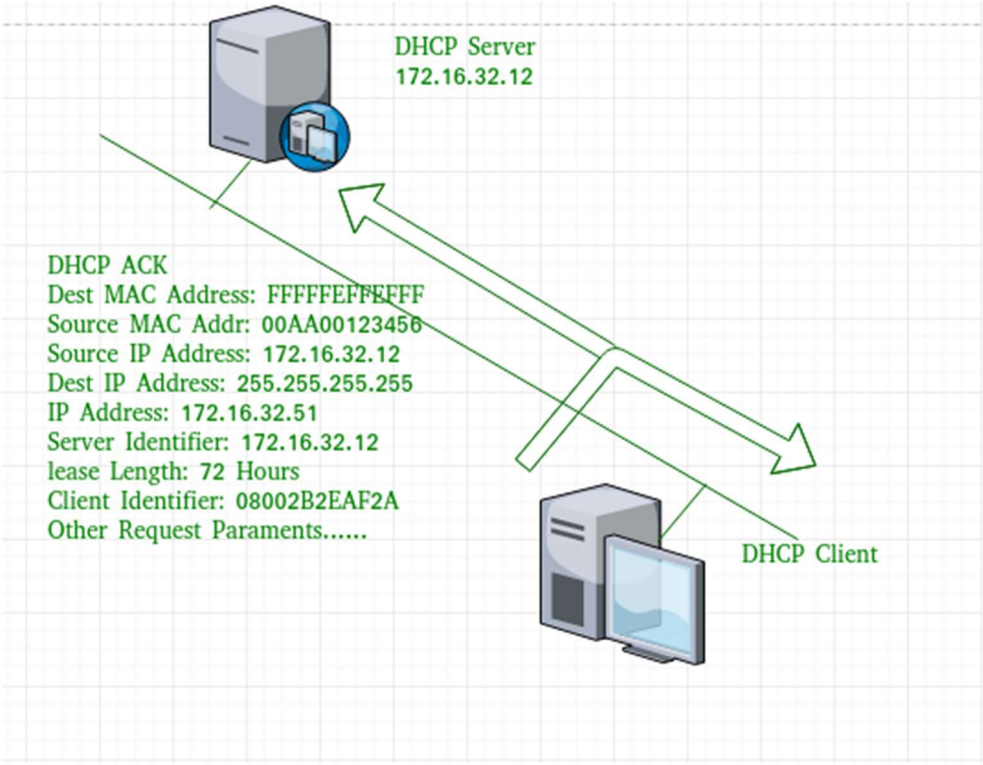


DHCP request message

Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (the broadcast IP address) and the source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

Note – This message is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request message for the server showing the acceptance of the IP address and Other TCP/IP Configuration.

4. DHCP acknowledgment message: In response to the request message received, the server will make an entry with a specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by the server.



DHCP acknowledgment message

Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by the server to any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

5. DHCP negative acknowledgment message: Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

6. DHCP decline: If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP release: A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

8. DHCP inform: If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration

suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.
Note – All the messages can be unicast also by the DHCP relay agent if the server is present in a different network.

Advantages of DHCP

- Centralized management of IP addresses.
- Centralized and automated TCP/IP configuration.
- Ease of adding new clients to a network.
- Reuse of IP addresses reduces the total number of IP addresses that are required.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.
- The DHCP protocol gives the network administrator a method to configure the network from a centralized area.
- With the help of DHCP, easy handling of new users and the reuse of IP addresses can be achieved.

Disadvantages of DHCP

- IP conflict can occur.
- The problem with DHCP is that clients accept any server. Accordingly, when another server is in the vicinity, the client may connect with this server, and this server may possibly send invalid data to the client.
- The client is not able to access the network in absence of a DHCP Server.
- The name of the machine will not be changed in a case when a new IP Address is assigned.

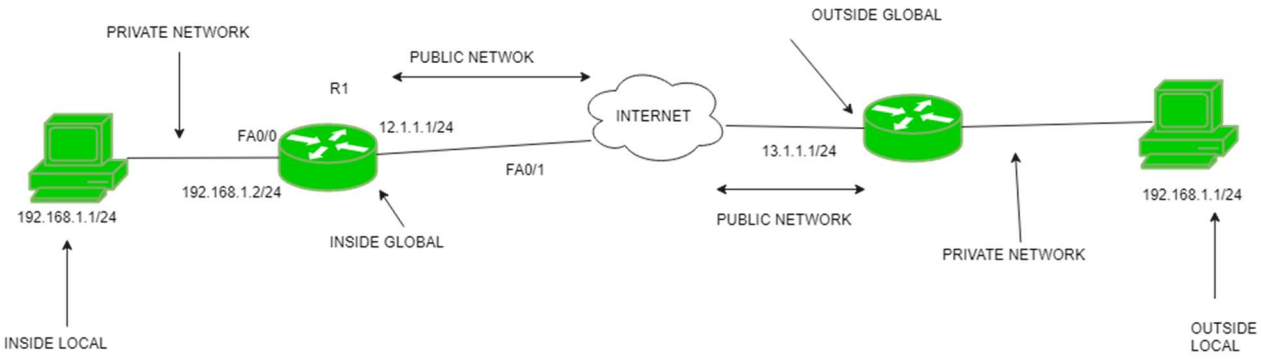
Network Address Translation(NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and

vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –
Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.
If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

NAT inside and outside addresses –
Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.

- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –
There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.
   Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
   Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

Internet Control Message Protocol(ICMP)

nternet Control Message Protocol is known as ICMP. The protocol is at the network layer. It is mostly utilized on network equipment like routers and is utilized for error handling at the network layer. Since there are various kinds of network layer faults, ICMP can be utilized to report and troubleshoot these errors.
Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide error control. In this article, we are going to discuss ICMP in detail along with their uses, messages, etc.

What is ICMP?

ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.
Since the IP protocol lacks an error-reporting or error-correcting mechanism, information is communicated via a message. For instance, when a message is sent to its intended recipient, it may be intercepted along the route from the

sender. The sender may believe that the communication has reached its destination if no one reports the problem. If a middleman reports the mistake,

Uses of ICMP

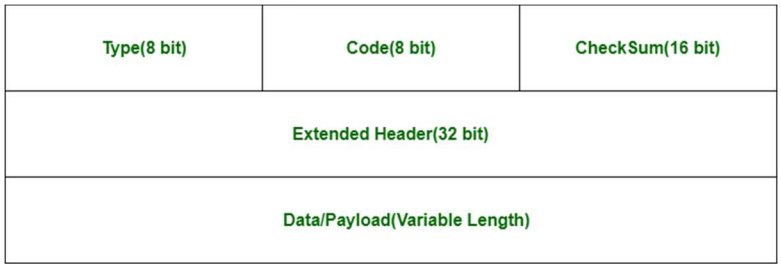
ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any message which is large enough for the receiver, in that case, the receiver will drop the message and reply to the ICMP message to the source.
Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility.
Traceroute: Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.

How Does ICMP Work?

ICMP is the primary and important protocol of the IP suite, but ICMP isn't associated with any transport layer protocol (TCP or UDP) as it doesn't need to establish a connection with the destination device before sending any message as it is a connectionless protocol.
The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake.
ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data. ICMP datagram is similar to a packet, which is an independent data entity.

ICMP Packet Format

ICMP header comes after IPv4 and IPv6 packet header.



ICMPv4 Packet Format

In the ICMP packet format, the first 32 bits of the packet contain three fields:

Type (8-bit): The initial 8-bit of the packet is for message type, it provides a brief description of the message so that receiving network would know what kind of message it is receiving and how to respond to it. 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): Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type.

Checksum (16-bit): Last 16 bits are for the checksum field in the ICMP packet header. The checksum is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.

The next 32 bits of the ICMP Header are Extended Header which has the work of pointing out the problem in IP Message. Byte locations are identified by the pointer which causes the problem message and receiving device looks here for pointing to the problem.

The last part of the ICMP packet is Data or Payload of variable length. The bytes included in IPv4 are 576 bytes and in IPv6, 1280 bytes.

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

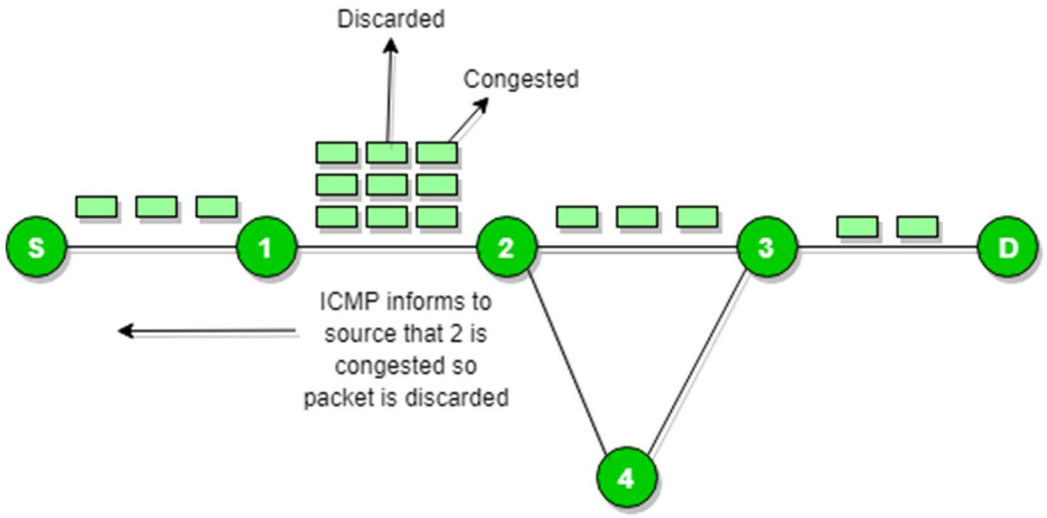
Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation is needed and the DF flag set
	5	Source route failed
5 – Redirect Message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

Type	Code	Description
	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

Type	Code	Description
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

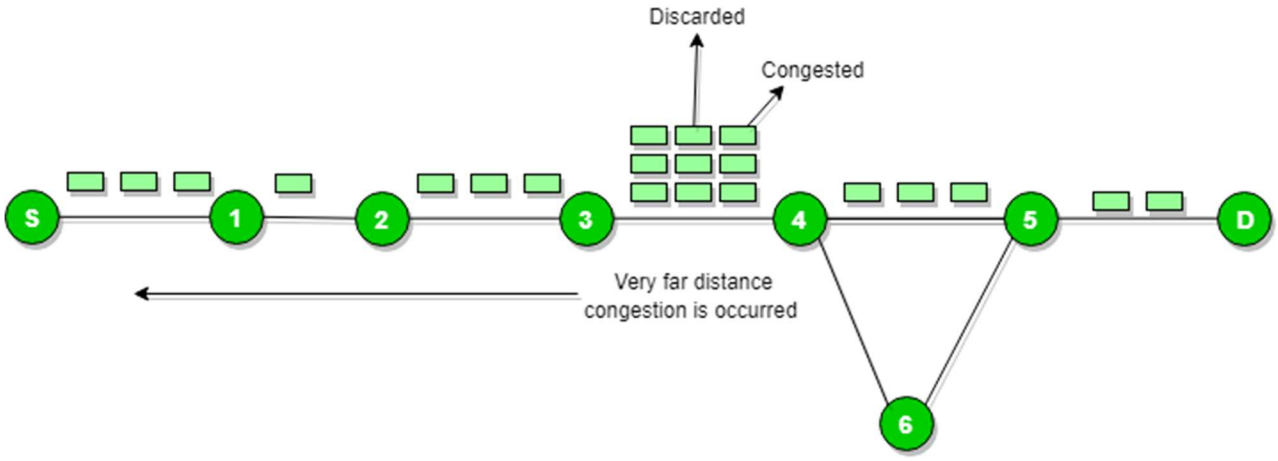
Source Quench Message

A source quench message is a request to decrease the traffic rate for messages sent to the host destination) or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.



Source Quench Message

ICMP will take the source IP from the discarded packet and inform the source by sending a source quench message. The source will reduce the speed of transmission so that router will be free from congestion.

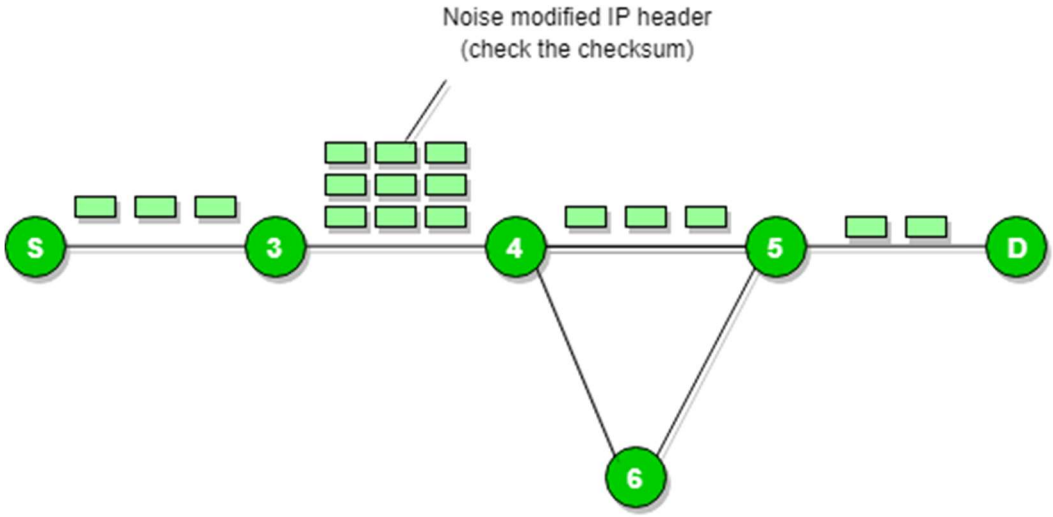


Source Quench Message with Reduced Speed

When the congestion router is far away from the source the ICMP will send a hop-by-hop source quench message so that every router will reduce the speed of transmission.

Parameter Problem

Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then only the packet is accepted by the router.

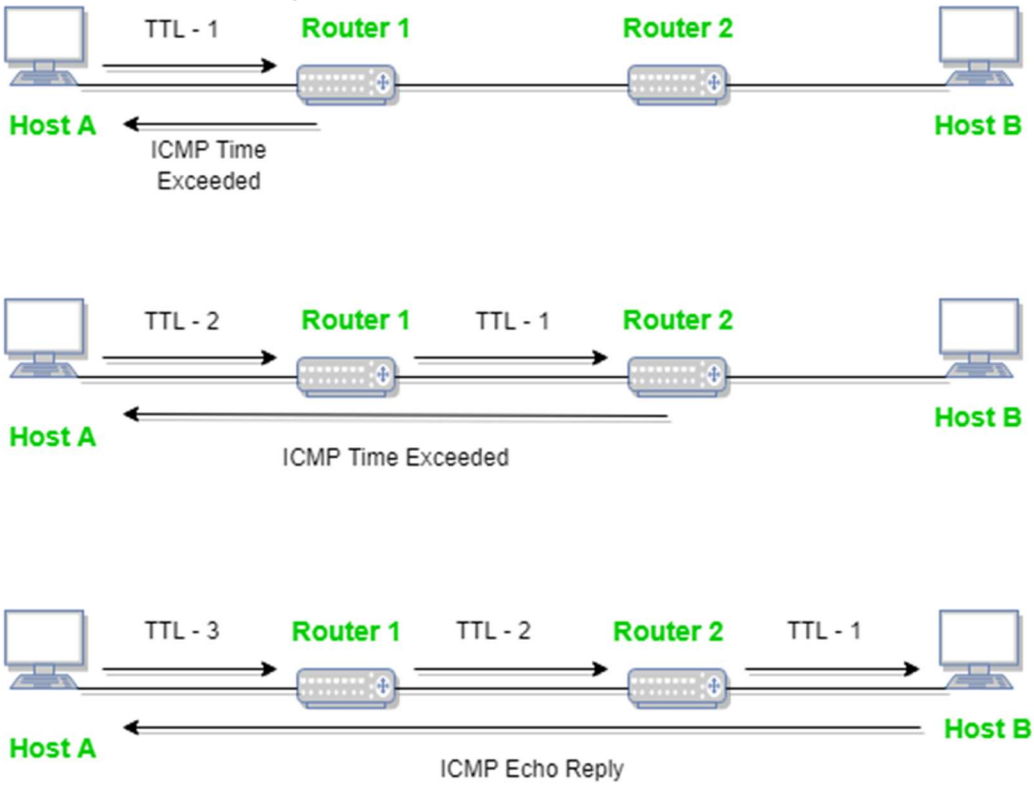


Parameter Problem

If there is a mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and inform the source by sending a parameter problem message.

Time Exceeded Message

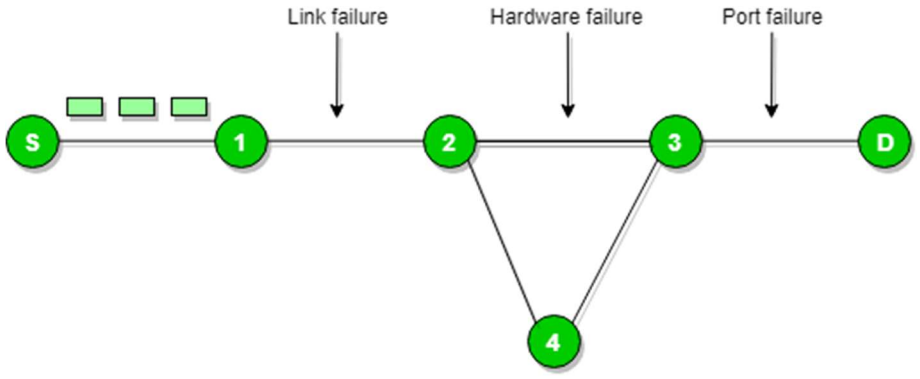


Time Exceeded Message

A notification with the subject line “Time Exceeded” is typically generated by routers or gateways. You need to know what an IP header is in a packet in order to comprehend this ICMP message in its entirety. The IP protocol structure is covered in great detail in the section on IP Protocol, which is freely available to our readers.

Destination Un-reachable

The destination is unreachable and is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



Destination Un-reachable

There is no necessary condition that only the router gives the ICMP error message time the destination host sends an ICMP error message when any type of failure (link failure, hardware failure, port failure, etc) happens in the network.

Redirection Message

Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information (to send packets on an alternate route).

Example: If the host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from the host to R2. Then R1 will send a redirect message to inform the host that there is the best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.

The router R2 will send the original datagram to the intended destination. But if the datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

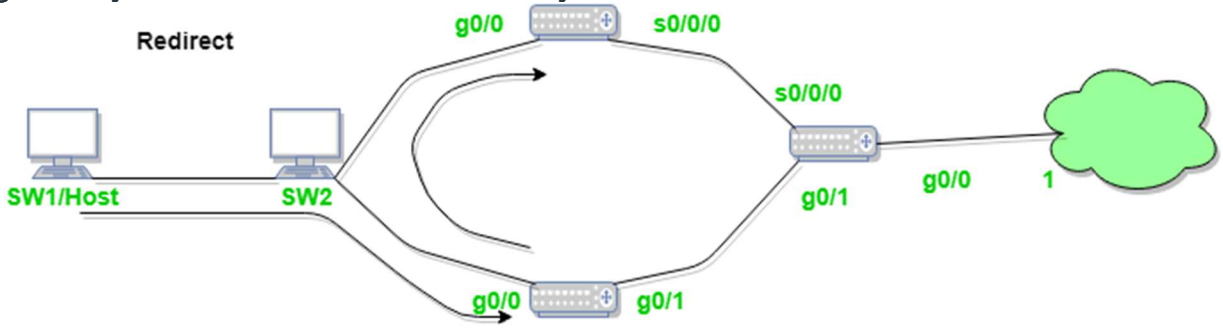


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

Redirection Message

Whenever a packet is forwarded in the wrong direction later it is re-directed in a current direction then ICMP will send a re-directed message.

For more, you can refer to Types of ICMP (Internet Control Message Protocol) Messages.

Advantages of ICMP

- Network devices use ICMP to send error messages, and administrators can use the Ping and Tracert commands to debug the network.
- These alerts are used by administrators to identify issues with network connectivity.
- A prime example is when a destination or gateway host notifies the source host via an ICMP message if there is a problem or a change in network connectivity that needs to be reported. Examples include when a destination host or networking becomes unavailable, when a packet is lost during transmission, etc.
- Furthermore, network performance and connection monitoring tools commonly employ ICMP to identify the existence of issues that the network team has to resolve.
- One quick and simple method to test connections and find the source is to use the ICMP protocol, which consists of queries and answers.

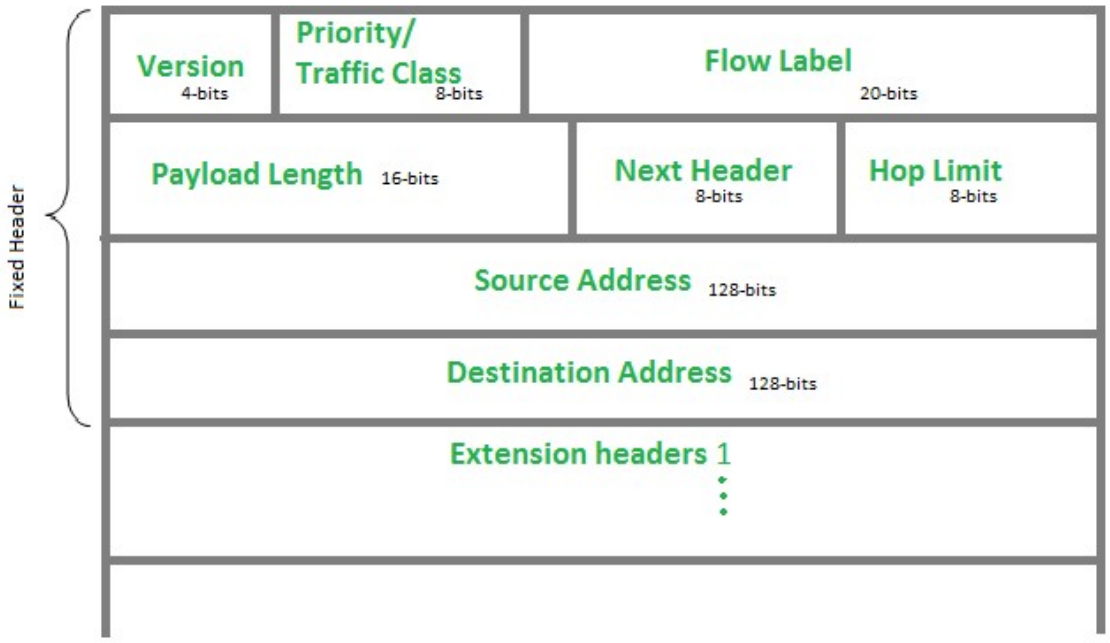
Disadvantages of ICMP

- 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.

IPv6 Header:

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

IP version 6 Header Format :



Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.
Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.
As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
Priority assignment of Congestion controlled traffic :

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.
Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.
Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.
Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed

to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

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

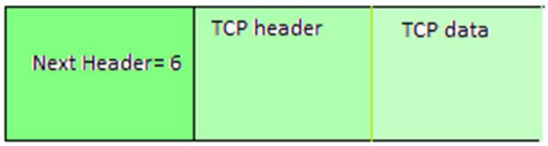
Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

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

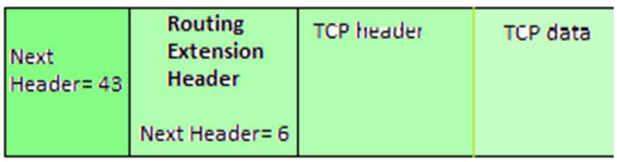
IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*



Example2:



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

Conventions :

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

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

Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

Moving from IPv4 to IPv6: tunnelling,

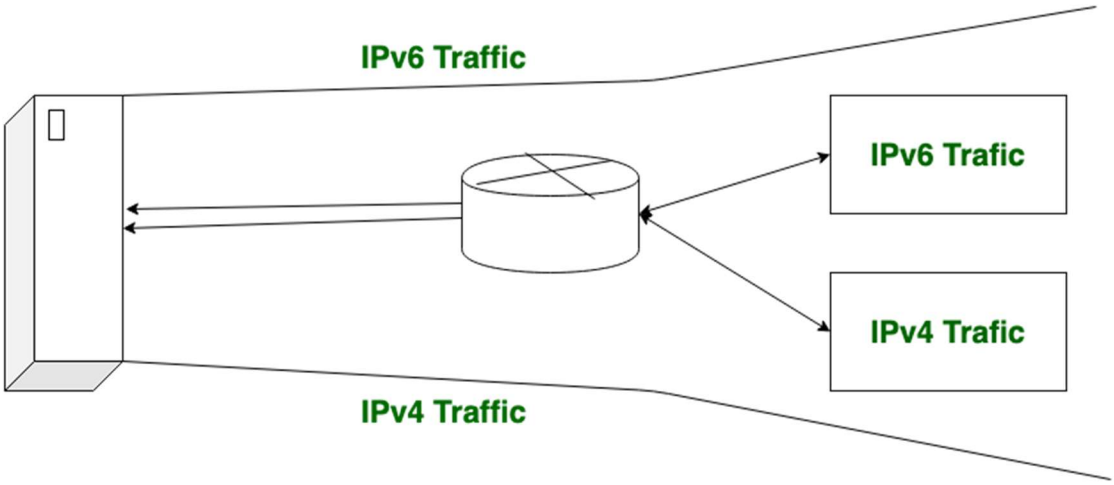
In the current scenario, the IPv4 address is exhausted and IPv6 had come to overcome the limit.

Various organization is currently working with IPv4 technology and in one day we can't switch directly from IPv4 to IPv6. Instead of only using IPv6, we use combination of both and transition means not replacing IPv4 but co-existing of both.

When we want to send a request from an IPv4 address to an IPv6 address, but it isn't possible because IPv4 and IPv6 transition is not compatible. For a solution to this problem, we use some technologies. These technologies are *Dual Stack Routers, Tunneling, and NAT Protocol Translation*. These are explained as following below.

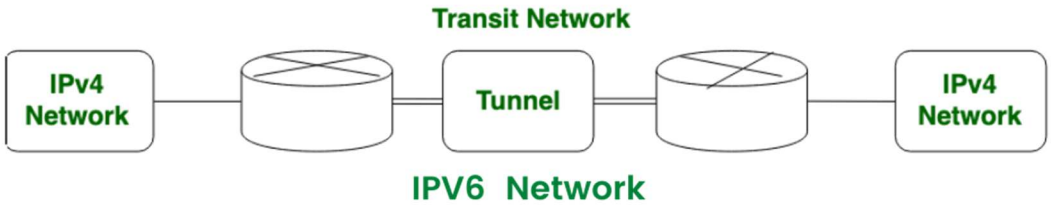
1. Dual-Stack Routers:

In dual-stack router, A router's interface is attached with IPv4 and IPv6 addresses configured are used in order to transition from IPv4 to IPv6.



In this above diagram, A given server with both IPv4 and IPv6 addresses configured can communicate with all hosts of IPv4 and IPv6 via dual-stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with the server without changing their IP addresses.

2. Tunneling:
Tunneling is used as a medium to communicate the transit network with the different IP versions.



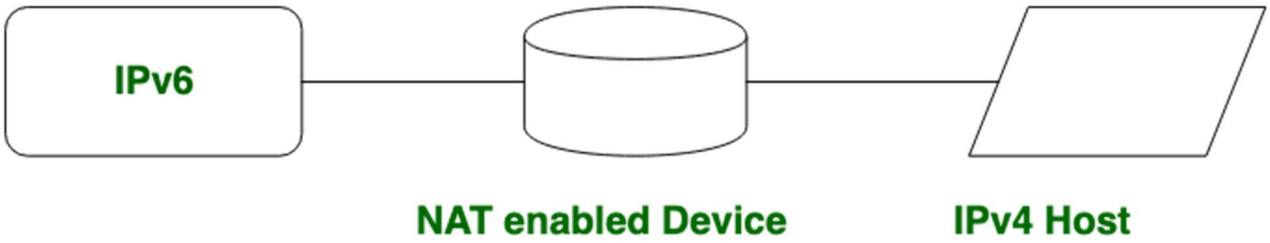
In this above diagram, the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of the Tunnel. It's also possible that the IPv6 network can also communicate with IPv4 networks with the help of a Tunnel.

3. NAT Protocol Translation:

With the help of the NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.

Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which removes the header of first (sender) IP version address and add the second

(receiver) IP version address so that the Receiver IP version address understand that the request is sent by the same IP version, and its vice-versa is also possible.



In the above diagram, an IPv4 address communicates with the IPv6 address via a NAT-PT device to communicate easily. In this situation, the IPv6 address understands that the request is sent by the same IP version (IPv6) and it responds.