Module 6

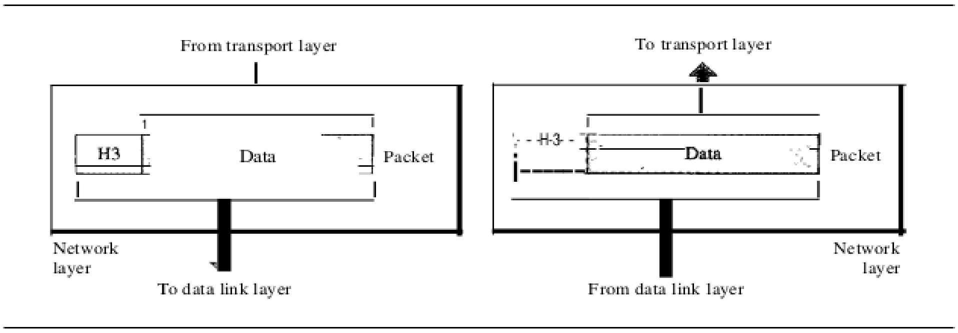
The Network Layer

- Store-and-forward packet switching Services Provided to the Transport Layer,
- Implementation of Connectionless Service,
- Implementation of Connection Oriented Service
- Comparison of Virtual Circuit and Datagram
- IPV4, IPV6
- Addresses – Address Space Notations, Classful Addressing, Subnetting, Supernetting,Classless Addressing,
- Datagram Format, Fragmentation, Checksum, Options.

The Netwok Layer :

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.
- If two systems are connected to the same link, there is usually no need for a net- work layer.
- However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

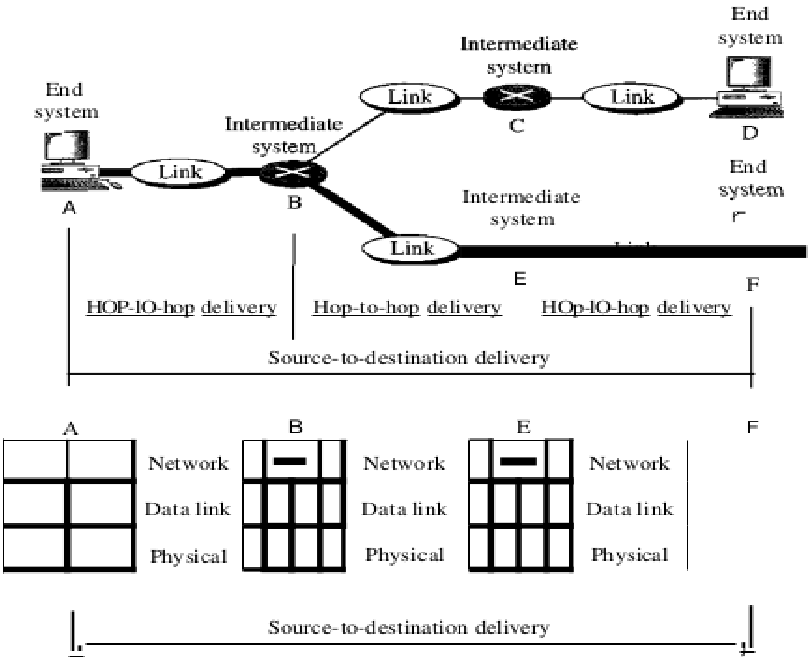


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

i. Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

ii. Routing. When independent networks or links are connected to create intemetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the func-tions of the network layer is to provide this mechanism.



As the figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.

What are services provided to transport layer by network layer?

The network layer is concerned with getting packets from the source all the way to the destination with minimal cost. Unlike the data link layer which has more important goals like just moving frames from one end of a wire to another. The network layer is the lowest layer that deals with end-to-end transmission.

Network layer Design issues are as follows −

- Store and forward packets switching
- Services provided to the transport layer
- Implementation of connectionless services
- Implementation of connection oriented services
- Comparison of virtual-circuit datagram networks

Services provided to the transport layer

The services provided to the transport layer are as follows −

Logical Addressing− Network layer adds header to incoming packet which includes logical address to identify sender and receiver.

Routing− It is the mechanism provided by Network Layer for routing the packets to the final destination in the fastest possible and efficient way.

Flow control− This layer routes the packet to another way, If too many packets are present at the same time preventing bottlenecks and congestion.

Breaks Large Packets− Breaks larger packets into small packets.

Connection Oriented service− It is a network communication mode, where a communication session is established before any useful data can be transferred and where a stream of data is delivered in the same order as it was sent.

Connectionless Service− It is a data transmission method used in packet switching networks by which each data unit is individually addressed and routed based on information carried in each unit, rather than in the setup information of a prearranged, fixed data channel as in connection-oriented communication.

DataGram− A datagram is a basic transfer unit associated with a packet-switched network. The delivery, arrival time and order of arrival need not be guaranteed by the network.

A virtual circuit− It is a means of transporting data over a packet switched computer network in such a way that it appears as though there is a dedicated physical layer link between the source and destination end system of this data.

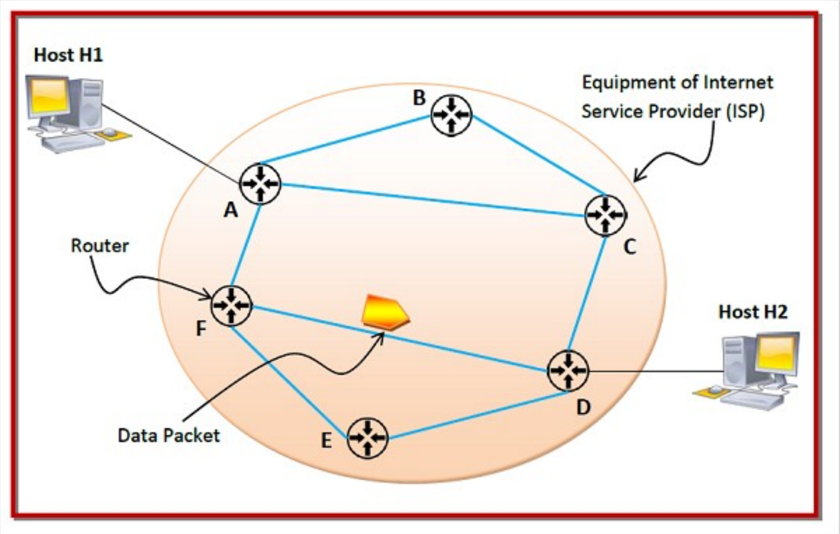
Store – and – Forward Packet Switching

- In telecommunications, store − and − forward packet switching is a technique where the data packets are stored in each intermediate node, before they are forwarded to the next node.
- The intermediate node checks whether the packet is error−free before transmitting, thus ensuring integrity of the data packets.
- In general, the network layer operates in an environment that uses store and forward packet switching.
-

Working Principle

- The node which has a packet to send, delivers it to the nearest node, i.e. router.
- The packet is stored in the router until it has fully arrived and its checksum is verified for error detection.
- Once, this is done, the packet is transmitted to the next router.
- The same process is continued in each router until the packet reaches its destination.

The following scenario exemplifies the mechanism −



In the above diagram, we can see that the Internet Service Provider (ISP) has six routers (A to F) connected by transmission lines shown in blue lines. There are two hosts, host H1 is connected to router A, while host H2 is connected to router D. Suppose that H1 wants to send a data packet to H2. H1 sends the packet to router A. The packet is stored in router A until it has arrived fully. Router A verifies the checksum using CRC (cyclic redundancy check) code. If there is a CRC error, the packet is discarded, otherwise it is transmitted to the next hop, here router F. The same process is followed by router F which then transmits the packet to router D. Finally router D delivers the packet to host H2.

Advantages and Disadvantages

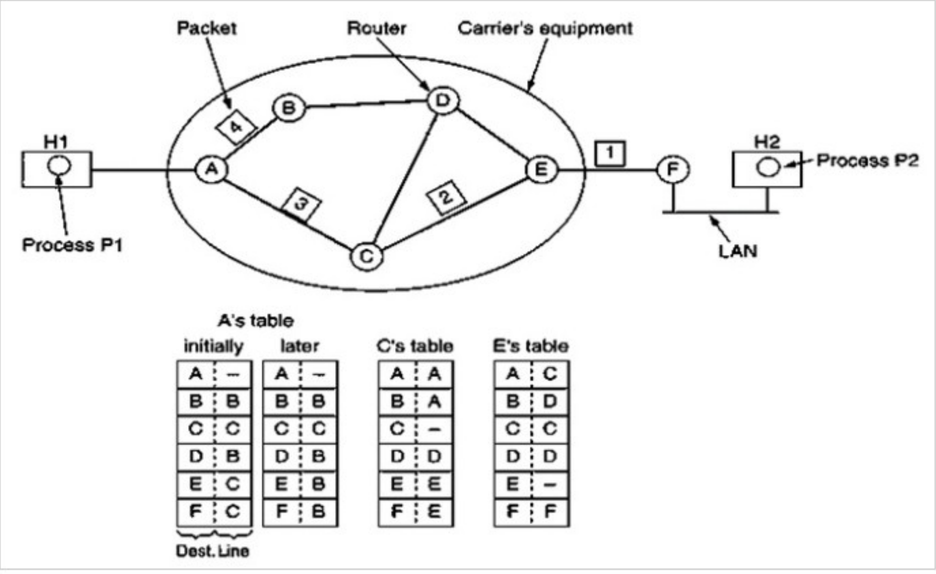
Store − and forward packet switching ensures high quality data packet transmission. Since erroneous packets are discarded at each router, bad packets or invalid packets in the network are mostly eliminated.

However, error − free packet transmission is achieved by compromising on the overall speed of transmission. Switch latency is introduced due to waiting for entire packet to arrive as well as computation of CRC. Though the latency at each router may seem small enough, the cumulative latency at all routers make it inappropriate for time − critical online applications.

Implementation of connection less services

- A Connectionless Service is technique that is used in data communications to send or transfer data or message at Layer 4 i.e., Transport Layer of Open System Interconnection model. This service does not require session connection among sender or source and receiver or destination. Sender starts transferring or sending data or messages to destination.
- In other words, we can say that connectionless service simply means that node can transfer or send data packets or messages to its receiver even without session connection to receiver. Message is sent or transferred without prior arrangement. This usually works due to error handling protocols that allow and give permission for correction of errors just like requesting retransmission.
- In this service, network sends each packet of data to sender one at a time, independently of other packets. But network does not have any state information to determine or identify whether packet is part of stream of other packets. Even the network doesn’t have any knowledge and information about amount of traffic that will be transferred by user. In this, each of data packets has source or destination address and is routed independently from source to destination.
- Therefore, data packets or messages might follow different paths to reach destination. Data packets are also called datagrams. It is also similar to that of postal services, as it also carries full address of destination where message is to send. Data is also sent in one direction from source to destination without checking that destination is still present there or not or if receiver or destination is prepared to accept message.
- When connectionless service is offered, packets are frequently called Datagrams (just like telegrams) because individual packets are injected to the subnet and are routed individually.
- No advance setup is required. Subnets are called Datagram subnets. When Connection

oriented service is provided, then before any packet is sent a path from source router to destination router is established. This connection is called Virtual Circuit and the subnet is called Virtual Circuit subnet.



A's table

initially		later		C's table		E's table	
A	–	A	–	A	A	A	C
B	B	B	B	B	A	B	D
C	C	C	C	C	–	C	C
D	B	D	B	D	D	D	D
E	C	E	B	E	E	E	–
F	C	F	B	F	E	F	F

Dest. Line

Datagram Network

Let us discuss how datagram network works in stepwise manner −

- **Step 1** − Suppose there is a process P1 on host H1 and is having a message to deliver to P2 on host H2. P1 hands the message to the transport layer along with instructions to be delivered to P2 on H2.

- **Step 2** − Transport Layer code is running on H1 and within the operating system. It prepends a transport header to the message and the end result is given to the network layer.

- **Step 3** − Let us assume for this example a packet which is four times heavier than the maximum size of the packet, then the packet is broken to four different packets and each of the packet is sent to the router A using point to point protocol and from this point career takes over.

- **Step 4** − Each router will have an internal table saying where packets to be sent. Every table entry is a pair consisting of a destination and outgoing line to use for that destination. Only directly connected lines can be used.

- **Step 5** − For example A has only two outgoing lines to B and C, therefore every incoming packet must be sent to one of these routers, even if the ultimate destination will be some other router.

- **Step 6** − As the packets arrived at A, packet 1,2,3 and 4 were stored in brief. Then every packet is moved to C as per A’s table. Packet 1 is forwarded to E and then moved to F. When packet 1 is moved to F, then it will be encapsulated in a data link layer and sent to H2 over to LAN. Packet 2 and 3 will also follow the same route.

- **Step 7 −** When packet 4 reaches A, then it was sent to router B, even if the destination was F. For some purpose A decided to send packet 4 through a different route. It was because of the traffic jam in ACE path and the routing table was updated. Routing Algorithm decides routes, makes routing decisions and manages routing tables.

Connectionless Protocols :

These protocols simply allow data to be transferred without any link among processes. Some Of data packets may also be lost during transmission. Some of protocols for connectionless services are given below:

Internet Protocol (IP) –

This protocol is connectionless. In this protocol, all packets in IP network are routed independently. They might not go through same route.

User Datagram Protocol (UDP) –

This protocol does not establish any connection before transferring data. It just sends data that’s why UDP is known as connectionless.

Internet Control Message Protocol (ICMP) –

ICMP is called connectionless simply because it does not need any hosts to handshake before establishing any connection.

Internetwork Packet Exchange (IPX) –

IPX is called connectionless as it doesn’t need any consistent connection that is required to be maintained while data packets or messages are being transferred from one system to another.

Types of Connectionless Services :

Service	Example
Unreliable Datagram	Electronic Junk Mail, etc.
Acknowledged Datagram	Registered mail, text messages along with delivery report, etc.
Request Reply	Queries from remote databases, etc.

Advantages :

- It is very fast and also allows for multicast and broadcast operations in which similar data are transferred to various recipients in a single transmission.
- The effect of any error occurred can be reduced by implementing error-correcting within an application protocol.
- This service is very easy and simple and is also low overhead.
- At the network layer, host software is very much simpler.
- No authentication is required in this service.
- Some of the application doesn't even require sequential delivery of packets or data. Examples include packet voice, etc.

Disadvantages :

- This service is less reliable as compared to connection-oriented service.
- It does not guarantee that there will be no loss, or error occurrence, misdelivery, duplication, or out-of-sequence delivery of the packet.
- They are more prone towards network congestions.

Implementation of connection-oriented services

- **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, that is designed and developed after telephone system.
- Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.

- 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).

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.

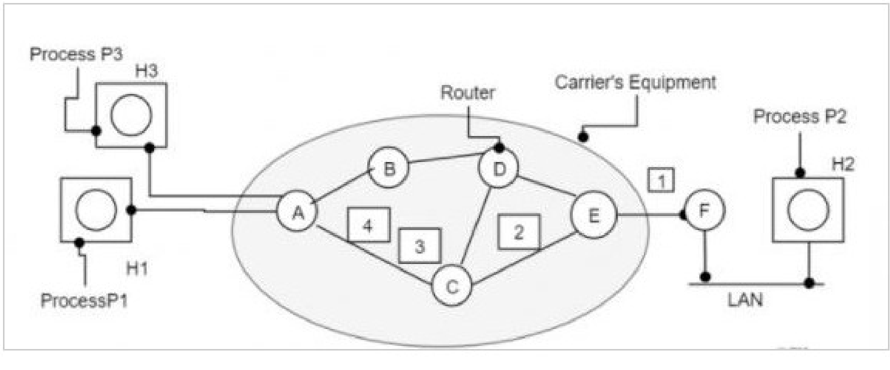
2. Transferring Data or Message – When this session connection is established, then we transfer or send message or data.

3. Releasing the Connection – After sending or transferring data, we release connection.

We need a virtual-circuit subnet for connection-oriented service. Virtual circuits were designed to avoid having to choose a new route for every packet sent.

- Instead, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers, when a connection is established. That route is utilised for all traffic flowing over the connection, and exactly the same manner even telephone works.
- The virtual circuit is also terminated, when the connection is released. In connection-oriented service, every packet will have an identifier which tells to which virtual circuit it belongs to.

The implementation of connection-oriented services is diagrammatically represented as follows −



Example

Consider the scenario as mentioned in the above figure.

- **Step 1** − Host H1 has established connection 1 with host H2, which is remembered as the first entry in every routing table.
- **Step 2** − The first line of A’s infers when packet is having connection identifier 1 is coming from host H1 and has to be sent to router W and given connection identifier as 1.
- **Step 3** − Similarly, the first entry at W routes the packet to Y, also with connection identifier 1.
- **Step 4** − If H3 also wants to establish a connection to H2 then it chooses connection identifier 1 and tells the subnet to establish the virtual circuit. This will be appearing in the second row in the table.
- **Step 5** − Note that we have a conflict here because although we can easily distinguish connection 1 packets from H1 from connection 1 packet from H3, W cannot do this.
- **Step 6** − For this reason, we assign a different connection identifier to the outgoing traffic for the second connection. Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.

Different Ways :

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

- **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.
- **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.
-
- Comparison of Virtual Circuit and Datagram

Computer networks that provide connection-oriented services are called Virtual Circuits while those providing connection-less services are called Datagram networks. For prior knowledge, the Internet which we use is actually based on a Datagram network (connection-less) at the network level as all packets from a source to a destination do not follow the same path.
Let us see what are the highlighting differences between these two hot debated topics here:

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 setup 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.

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.

IPv4 vs IPv6

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

- IPv4
- IPv6

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

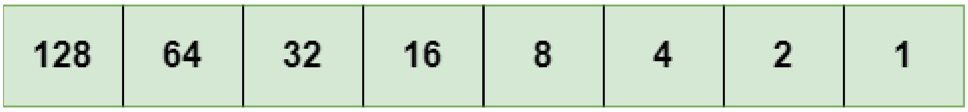
For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

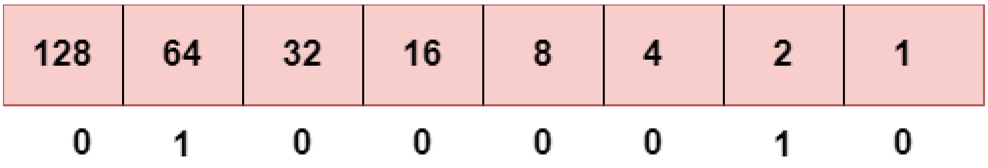


128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

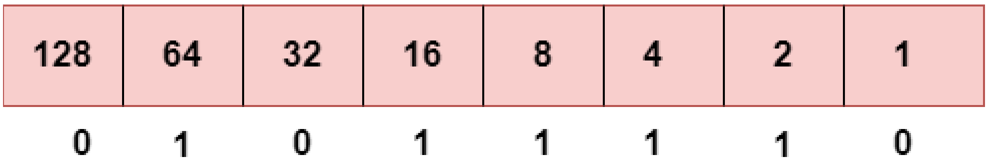
Step 1: First, we find the binary number of 66.



128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

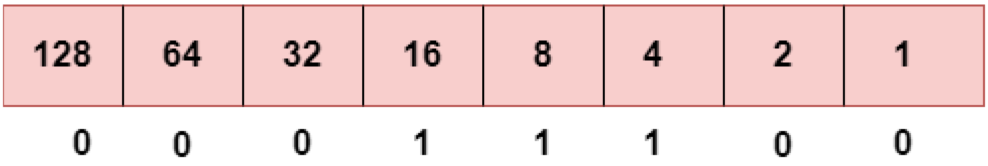
Step 2: Now, we calculate the binary number of 94.



128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

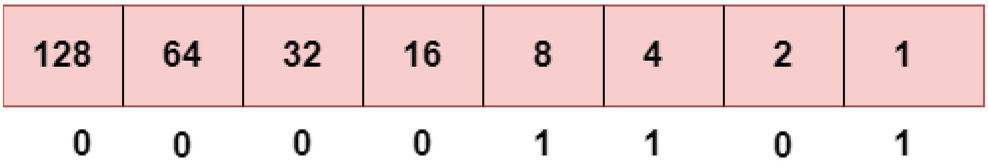
Step 3: The next number is 29.



128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.



128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

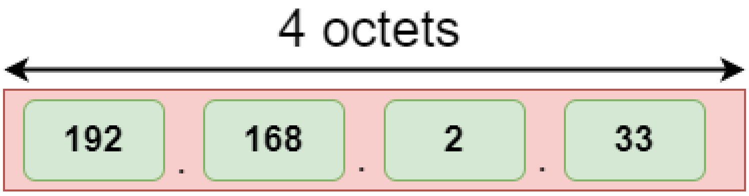
- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion ($3.4*10^{38}$) addresses.

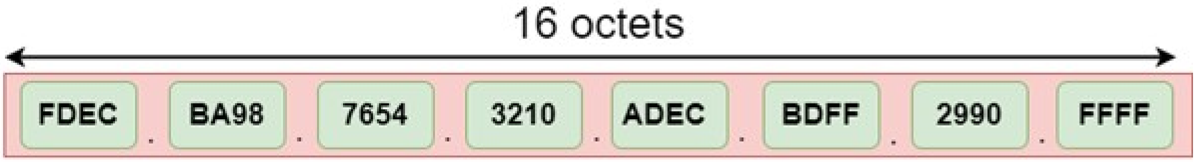
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the	Fragmentation is done by the

	senders and the forwarding routers.	senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

Addresses – Address Space Notations, Classful Addressing, Subnetting, Supernetting, Classless Addressing,

Address Space

Network supports classless IP addressing, also known as variable length subnet masking. These sets of addresses are called "address spaces". One or many address spaces may be grouped into a Network record which corresponds with an actual network. For example, the Ivory Tower building has one network which contains 2 address spaces -- 171.64.60.0/24 (the regular address space) and 172.24.60.0/24 (private address space).

Address spaces are generally specified with 2 parameters:

- **Network Number** - first address in the address space Example: 171.64.60.10, 128.12.75.2, 172.24.60.10

•**Subnet mask or Network Prefix Length**- determines size of address space by specifying division between network ID and host ID

•subnet mask 32 bit number expressed as 4 decimal numbers separated by dots examples: 255.0.0.0, 255.255.0.0

•network prefix length front slash with decimal number specifying how many bits are in the network ID sometimes called "slash notation" examples: /24, /23

Subnet Mask	Prefix Length	Addresses
255.255.252.0	/22	1024
255.255.254.0	/23	512
255.255.255.0	/24	256
255.255.255.128	/25	128
255.255.255.192	/26	64
255.255.255.224	/27	32
255.255.255.240	/28	16
255.255.255.248	/29	8

Classful Address

The first addressing system to be implemented as part of the Internet Protocol was Classful Addressing. In the year 1981, the Classful addressing network architecture was first used on the Internet. The Classful addressing system was superseded by a Classless addressing scheme with the introduction of Classless Inter-Domain Routing (CIDR) in 1993.

•The IP address comprises up of 32 bits and is split into four sections separated by dots:**part 1, part 2, part 3, and part 4**.

•The IP address is made up of four parts, each of which is eight bits long (1 byte).

•Further, the 4 parts of the IP address is divided into parts: a **network ID** and a **Host ID**.

Types of Classful Address

Class A, Class B, Class C, Class D, and Class E are the five varieties of Classful addresses. In IPv4, this classification is known as Classful addressing or IP address classes.

- The first three classes, Class A, B, and C, are used for "public addressing", in which communication is always one-to-one between source and destination. It implies that when data is transmitted from a source, it will only be sent to a single network host.
- The reserved categories include Class D and Class E, with Class D being utilized for multicast and Class E being saved for future usage exclusively.
- In IPv4, the Network ID is the first part of Class A, B, and C, while the Host ID is the remaining second portion.
- The Host ID always indicates the number of hosts or nodes in a certain network, whereas the Network ID always identifies the network in a specific place.
- In Class A, B, and C, the address space is split into a certain number of IP address blocks. It also specifies the maximum number of hosts in a network.

Network and Host part in Classful Addressing

The first octet or byte of an IP address is part of the network ID (short for Net-ID), while the next three octets or three bytes are part of the host ID in Class A. (in short, host-ID).

- The network ID takes up the first two octets or two bytes in Class B, whereas the host ID takes up the remaining two octets or two bytes.
- In Class C, the first three octets or bytes are dedicated to the network ID, while the last octet or byte is dedicated to the host ID.

Classless Addressing

Classless Inter-Domain Routing (CIDR) is another name for classless addressing. This addressing type aids in the more efficient allocation of IP addresses. This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses. This block is known as a "CIDR block", and it contains the necessary number of IP addresses.

When allocating a block, classless addressing is concerned with the following three rules.

- **Rule 1** – The CIDR block's IP addresses must all be contiguous.
- **Rule 2** – The block size must be a power of two to be attractive. Furthermore, the block's size is equal to the number of IP addresses in the block.
- **Rule 3** – The block's first IP address must be divisible by the block size.

For example, assume the classless address is 192.168.1.35/27.

- The network component has a bit count of 27, whereas the host portion has a bit count of 5. (32-27)
- The binary representation of the address is: (00100011 . 11000000 . 10101000 . 00000001).
- (11000000.10101000.00000001.00100000) is the first IP address (assigns 0 to all host bits), that is, 192.168.1.32
- (11000000.10101000.00000001.00111111) is the most recent IP address (assigns 1 to all host bits), that is, 192.168.1.63
- The IP address range is 192.168.1.32 to 192.168.1.63.

Difference Between Classful and Classless Addressing

- Classful addressing is a technique of allocating IP addresses that divides them into five categories. Classless addressing is a technique of allocating IP addresses that is intended to replace classful addressing in order to reduce IP address depletion.
- The utility of classful and classless addressing is another distinction. Addressing without a class is more practical and helpful than addressing with a class.
- The network ID and host ID change based on the classes in classful addressing. In classless addressing, however, there is no distinction between network ID and host ID. As a result, another distinction between classful and classless addressing may be made.

Subnetting and Supernetting

Introduction to Subnetting and Supernetting

What is Subnetting?

- Subnetting is a technique that is used to divide the individual physical network into a smaller size called sub-networks. These sub-networks are called a subnet. An internal address is made up of a combination of the small networks segment and host segment. A subnetwork is designed by accepting the bits from the IP address host portion; then, they are uses to assign a number of small-sized sub-networks in the original network.
- In the subnetting process, network bits are converted into host bits. Subnetting process is performed to slow down the depletion of the IP addresses. It allows the administrator to divide the single class A, class B and class C into small segments. Subnetting makes use of VLSM (Variable Length Subnet Mask) and FLSM (Fixed Length Subnet Mask). The process of partitioning the IP address space into a subnet of different size is called a Variable Length Subnet Mask. VLSM reduces the wastage of memory. The process of partitioning the IP address space into a subnet of the same size is called a Fixed Length Subnet Mask.

Advantages and Disadvantages of Subnetting:

Below are some advantages and disadvantage of subnetting:

Advantages:

- Subnetting increases the number of allowed hosts in the local area network.
- Subnetting decreases the volume of broadcast, hence minimize the number of network traffic.
- Sub networks are easy to maintain and manage.
- Subnetting increases the flexibility of address.
- Network security can be readily employed between sub networks rather than employing it in the whole network.

Disadvantages:

- The process of subnetting is quite expensive.
- To perform subnetting process, we need a trained administrator.

What is Supernetting?

Supernetting is the process that is used to combine several sub networks into a single network. Its process is inverse of the subnetting process. In supernetting, mask bits are moved towards the left of the default mask; network bits are converted into hosts bits. Supernetting is also called router summarization and aggregation. It creates a more number of host addresses at the expense of network addresses. The Internet service provider performs the supernetting process to achieve the most efficient IP address allocation.

It uses the CIDR method, i.e. Classless inter-domain routing method, to route the network traffic across the internet. CIDR combines several sub networks and combined them together for routing network traffic. In other words, we can say that CIDR organizes the IP Addresses in the sub networks independent of the value of the Addresses.

Advantages and Disadvantages of Supernetting:

Below are some advantages and disadvantage of supernetting:

Advantages:

- Supernetting reduces the traffic of the network over the internet.
- Supernetting increases the speed of routing table lookup.
- As it is summarized the number of routing information entries into a single entry, the size of the router's memory table decreased, hence saving the memory space.
- Provision for the router to isolate the topology changes from the other routers.

Disadvantages:

- The combination of blocks should be made in power 2 alternatively; if the three blocks are required, then there must be assigned four blocks.
- While merging several entries into one, it lacks covering different areas.
- The whole network must exist in the same class.

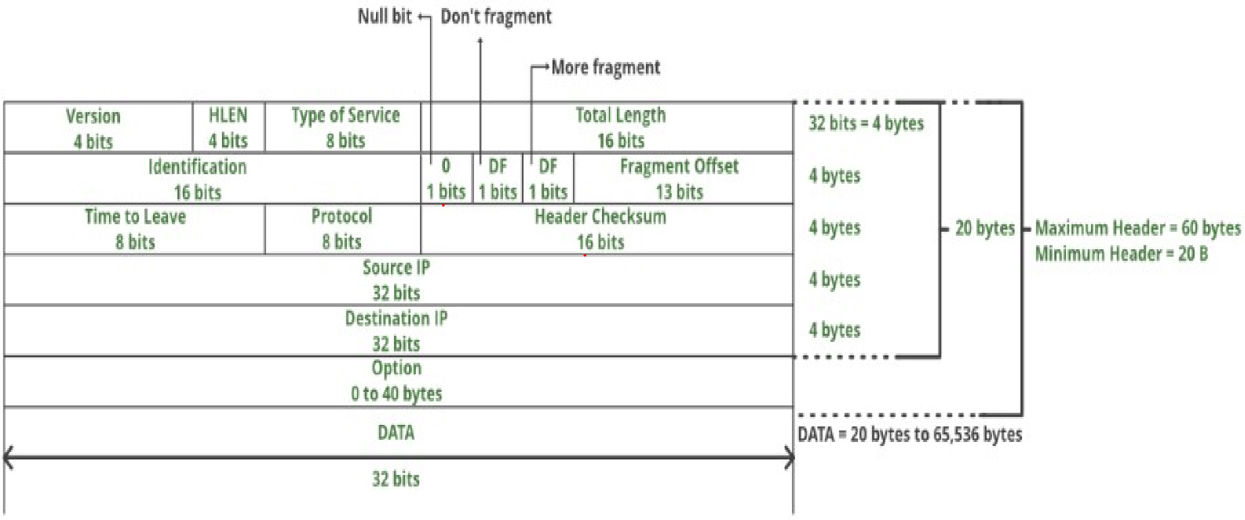
Difference Between Subnetting and Supernetting

- Subnetting divides the whole network into sub networks while supernetting combines the sub network and merge it as a whole network.
- Subnetting converts the bits of a host to bits of network hence increase the number of network bits, while supernetting converts the bits of a network to bits of the host, hence increase the number of host bits.

- Subnetting reduces the depletion of address, while supernetting increases the routing process.
- Subnetting uses VLSM and FL techniques, while supernetting uses CIDR.
- In subnetting, mask bits are moved towards the right of the default mask, whereas in supernetting, the mask bits are moved towards the left of the default mask.

Datagrams:

Packets in the network (internet) layer are called datagrams. Following figure shows the IP datagram format. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



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.

Reference Link

https://web.stanford.edu/group/networking/netdb/help/prodaddress_space.html

https://www.ripe.net/about-us/press-centre/understanding-ip-addressing

https://www.geeksforgeeks.org/difference-between-subnetting-and-supernetting/#:~:text=Subnetting%20is%20implemented%20via%20Variable,implemented%20via%20Classless%20interdomain%20routing.&text=1.,of%20combine%20the%20small%20networks.

https://users.cs.jmu.edu/aboutams/Web/Networking/Spring03/Lectures/Lecture%204-%20Sub_Supernetting%20and%20Classless%20Addressing.pdf

https://www.auvik.com/franklyit/blog/classful-classless-addressing/

https://www.geeksforgeeks.org/fragmentation-network-layer/

https://www.cs.dartmouth.edu/~campbell/cs60/ip-addressing.pdf

IPv4 → Class A
→ Class B
→ Class C
→ Class D
→ Class E

How to find class of an Address

0 - 255

Binary Notation

class A : 0......

B : 10.....

C : 110.....

D : 1110....

E : 1111....

Dotted Decimal

class A : 0-127

B : 128-191

C : 192-223

D : 224 : 239

E : 240-255

Dotted Decimal :→

i) 227.12.14.87 : class D

ii) 193.14.56.22 : class C

iii) 14.23.120.8 : class A

iv) 252.5.15.111 : class E

Binary Notation :

i) 00000001 00...... → class A

ii) 11000001 1000 .... class C

iii) 10100111 110 - - . class B

iv) 11110011 100 .... class E

class A

B

C

D

E