Module 3

Network Layer:
Network Layer Design issues, store and forward packet switching, connectionless and connection-oriented networks. **Routing algorithms** - optimality principle & shortest path. Congestion control algorithms, IPv4 vs IPv6 Protocol.

KEY FACTORS OF NETWORK LAYER

Network Layer Design Issues:

The network layer, the third layer of the OSI model, plays a critical role in facilitating communication between devices across different networks. Several design issues and considerations are important in the network layer's design:

1. Routing: The network layer is responsible for routing data packets from the source to the destination. One key design issue is selecting and implementing routing algorithms that determine the best path for data packets based on factors like cost, distance, and congestion.

2. Addressing: The network layer assigns unique addresses to devices on the network, enabling them to be identified and located. Designing an efficient addressing scheme is crucial for scalability and hierarchical organization of networks.

3. Packet Forwarding: Network layer devices, such as routers, are responsible for packet forwarding. Efficient packet forwarding mechanisms and lookup tables are critical for fast and accurate data transmission.

4. Error Handling: Designing error detection and error correction mechanisms at the network layer is essential for ensuring the reliability of data transmission.

5. Fragmentation and Reassembly: The network layer may need to handle large data packets that must be fragmented into smaller pieces for transmission over networks with lower Maximum Transmission Unit (MTU) sizes. Proper fragmentation and reassembly mechanisms must be designed.

6. Congestion Control: Managing network congestion is a significant challenge. Designing congestion control algorithms and mechanisms to prevent network congestion and reduce its impact on performance is essential.

7. Security: Network layer security, including encryption, authentication, and access control, is a critical design consideration to protect data during transmission.

Store and Forward Packet Switching:

Store and forward packet switching is a method used in network communication, particularly in packet-switched networks. In this approach:

- Data packets are received at a network node (such as a router) and are temporarily stored in a buffer or memory.

- The network node examines the header of the incoming packet to determine the appropriate outgoing interface or next hop.

- The packet is forwarded to the next hop or outgoing interface only after it has been completely received and stored.

- This mechanism ensures that the entire packet is error-free before forwarding it, reducing the likelihood of errors in transit.

Store and forward packet switching is commonly used in networks with varying link speeds, where packets may need to be temporarily buffered to match the speed of the sending and receiving interfaces.

Connectionless and Connection-Oriented Networks:

Connectionless Networks:

- In a connectionless network, such as the Internet using IP (Internet Protocol), each data packet is treated independently.

- There is no setup phase before data transmission. Each packet is forwarded based on its destination address without establishing a dedicated connection path.

- Connectionless networks are simple, scalable, and suitable for transmitting small, non-time-sensitive packets.

- They are best suited for applications where low latency is more critical than guaranteed delivery.

Connection-Oriented Networks:

- In a connection-oriented network, such as those using protocols like TCP (Transmission Control Protocol), a dedicated connection is established between sender and receiver before data transmission begins.

- A setup phase involves handshaking and negotiation to establish parameters for data transfer, including reliability and flow control settings.

- Connection-oriented networks offer guaranteed delivery, error detection and correction, and in-order data delivery.

- They are suitable for applications that require reliable and ordered data transmission, such as web browsing, file transfer, and video streaming.

IP ADDRESSING

IP Addresses, or Internet Protocol addresses, are numerical labels assigned to devices connected to a computer network that uses the Internet Protocol for communication. IP addresses serve two primary purposes: host or network interface identification and location addressing.

There are two main versions of IP addresses in use today:

1. IPv4 (Internet Protocol version 4):

- Format: IPv4 addresses are 32-bit binary numbers typically expressed in dotted-decimal notation, consisting of four decimal numbers separated by periods (e.g., 192.168.1.1).

- Usage: IPv4 addresses are used extensively in the current Internet. However, due to address exhaustion, IPv4 is being gradually replaced by IPv6.

2. IPv6 (Internet Protocol version 6):

- Format: IPv6 addresses are 128-bit binary numbers, often expressed in hexadecimal notation, with eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

- Usage: IPv6 is designed to replace IPv4 due to the limited address space of IPv4. It provides a vastly larger number of unique addresses to accommodate the growing number of devices connected to the Internet.

Usage Scenarios for IP Addresses:

1. Host Identification: IP addresses uniquely identify network interfaces on devices. They are used to identify specific devices in a network, enabling data packets to be directed to the correct recipient.

2. Routing: IP addresses play a crucial role in routing data packets across networks. Routers use destination IP addresses to determine the next hop or path for forwarding packets.

3. Network Segmentation: IP addresses are used to segment networks into subnets. Subnetting allows for better network organization, security, and traffic management.

4. Network Services: IP addresses are associated with various network services and devices, such as DNS servers (resolving domain names to IP addresses), DHCP servers (assigning IP addresses dynamically to clients), and network appliances.

5. Geolocation: IP addresses can be used for geolocation purposes, helping identify the approximate physical location of a device or user.

6. Security: IP addresses are involved in security measures, including firewall rules, access control lists (ACLs), and intrusion detection systems.

7. IPv6 Transition: IPv6 addresses are essential for transitioning to the newer Internet Protocol version and ensuring compatibility with future network technologies.

Working of an IP Address

During web surfing, you often face internet connection problems which might be because of the problem from the server side or with the system's IP address. But how is the connection between your system and the internet service provider established?

In this part of the tutorial on what is an IP address, you will step-wise understand the connection method:

The following steps can help us walk through how our system gets connected to the internet and the role of IP address in it:

1. The first step begins with your system, smartphone, and other network devices establishing a connection between the network device (wi-fi), which would, in a way, indirectly connect your device with the internet.
2. If our device connects to the internet through our home network, then the connection is provided by the Internet Service Provider (ISP). In contrast, in the case of a professional location, it provides the network through the company network.
3. At this step, your system is provided with its IP address by the network.
4. The system's request for an internet connection goes through the ISP, where the requested information is routed back to the system using the IP address. As the ISP establishes the internet connection to our system, it is also responsible for assigning the IP address to your device.
5. The IP addresses assigned to the system are never consistent. They change each time you connect to the internet through the network (ISP). You can also contact your ISP to provide your system with a different IP address.
6. In case you are traveling or are out of your home network, the internet connection established to the system is provided by an alternative network (public wi-fi, airport hotspot, etc.), which assigns the system with a temporary IP address provided by the ISP of the location network.

Versions of IP Address

In accordance with the increase in the demand for IP addresses, the original IP address, i.e., IPv4 addresses, did not cover the requirement, so the establishment of IPv6 address was done which includes IP addresses that could easily satisfy the present demand and was sufficient for the future demand as well.

IPv4 Addresses

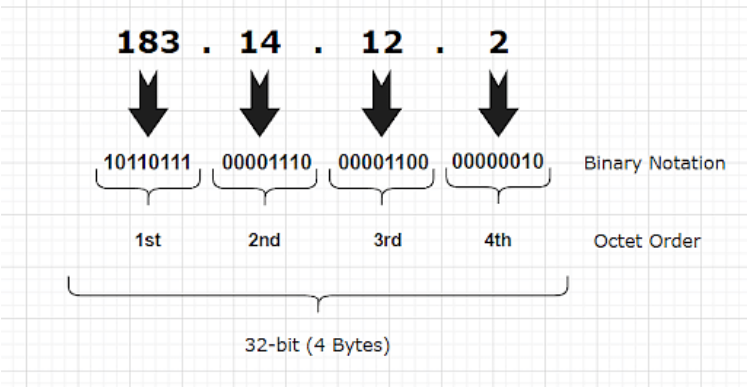

Fig 3.0 IPv4 Notation

This is the original version of the IP address, which was developed based on a 32-bit binary format and contained 232 addresses, which was sufficient at the initial time of making but somewhat lacking considering the increase in the current network advancement.

The addresses ranged from 0 to 255 in terms of 0s and 1s, with four octets, each of them separated by a period (.). The network device uses the binary format, whereas the numerical format is used for the host's reference.

IPv6 Addresses

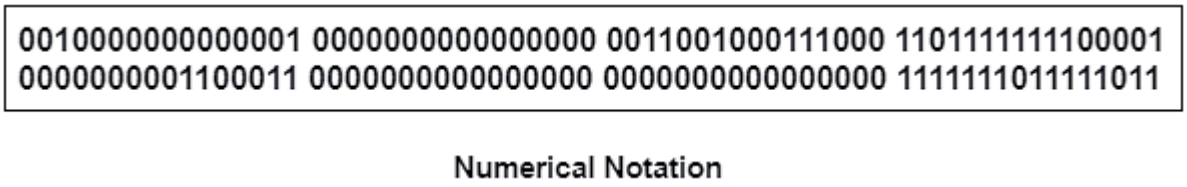

Fig 3.1 IPv6 Notation (Binary notation)

An IPv6 address is designed from 128 bits from which 4 hexadecimal digits and eight sets are created, with each block containing 16 bits separated by a colon (:).

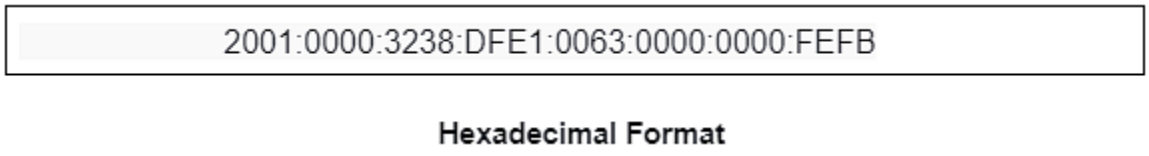

Fig 3.2 IPv6 Notation (Hexadecimal notation)

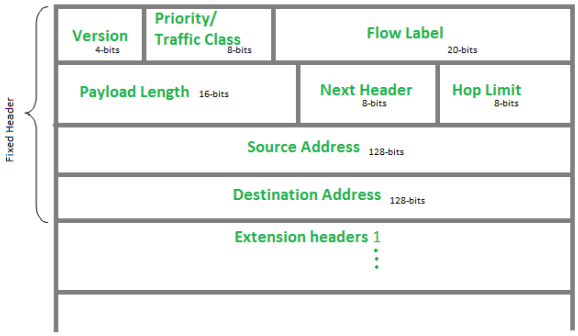

Fig 3.2.1 IPv6 datagram

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

Table 3.0 Explanation of IPv6 Format

IPv6 addresses are used to indicate the source and destination of each packet by including them in the packet header. The routing structure of the IP packets is assigned by using the IP address of the destination.

Consumer IP Addresses

The network connection, whether individual or professional with an active internet connection, follows two categories of IP addresses, i.e., Private IP addresses and Public IP addresses. Each of them is functional within their respective network locations, private IP addresses are accessible within the network, and public IP addresses function outside the network.

1. Private IP Addresses

The devices you connect to the internet network are all associated with the IP address, including laptops, computers, smartphones, etc. Also, with the advancement in the technology related to IoT(internet of things), the requirement for private IP addresses increased drastically. The network device (router) needs to identify the system individually. Then only the router would be able to generate private IP addresses for each of them to differentiate over the network.

2. Public IP Addresses

The public IP address acts as a whole primary address that contains all the other network devices associated with the network. Each device in the network is assigned its private IP address. The Internet Service Provider (ISP) supervises the assignment of the public IP address to the network device(router). ISPs accumulate a large number of IP addresses that they assign to their clients.

Public IP addresses can be further divided into two subcategories:

Dynamic IP Addresses

These types of IP addresses are the ones that are non-consistent and frequently changing. They are assigned by the ISPs from their large accumulation of IP addresses in accordance with the client's requirements. This way, frequently changing IP addresses prove to be cost-effective for the ISPs and also provide security from hackers and cybercriminals to a certain extent.

Static IP Addresses

As the name suggests, Static IP addresses are the type of constant addresses, unlike dynamic IP addresses. The IP address assigned to the system by the network device remains consistent. Due to the constant nature of the static IP address, companies and individuals avoid using static IP addresses. But they are required in case if a firm wants to assign a host to its network server.

The first eight bits of an IP address formerly identified the network that a particular host belonged to. This is known as classful addressing. This would have reduced the number of networks on the internet to only 254. These networks each had 16,777,216 unique IP addresses. The inefficiency of assigning IP addresses in this manner increased as the internet expanded.

After all, more than 254 companies require IP addresses, and even fewer networks require all 16.7 million available IP addresses.

An IP address is 32-bit long. An IP address is divided into sub-classes:

Class A

Class B

Class C

Class D

Class E

Components of IP Address

There are two components to an IP address:

1. Network ID: This identifies how many networks there are.
2. Host ID: This identifies how many hosts there are.

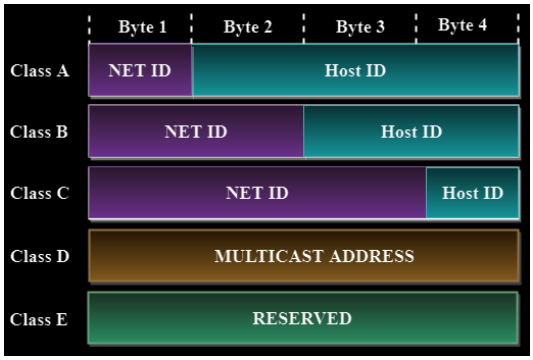

Fig 3.3 Components of IP Address

Advantages of Classful Addressing

1. We now understand that the long-term IP address answer to the IP address depletion issue is IPv6. IPv6 is not yet commonly utilized, yet.
2. It was obvious in the early 1990s that the IPv4 address space would quickly run out if nothing changed. As a result, classless addressing was employed as a temporary fix to assist us in extending the lifespan of IPv4.
3. Better use of IP address ranges. Classless addressing allowed for balanced use throughout what was once the Class A, B, and C ranges by separating the relationship between network size and IP address. Much fewer addresses were squandered.
4. Better directional planning. Route aggregation and classless routing protocols are made possible by VLSM and subnetting.

Different Classes and Properties

The five different types of Classful addresses are Class A, Class B, Class C, Class D, and Class E. This division is referred to as Classful addressing or IP address classes in IPv4.

1. In "public addressing," in which communication is always one-to-one between source and destination, the first three classes—Class A, B, and C—are employed. It suggests that when data is transferred from a source, only one network host will receive it.
2. Class D and Class E are among the reserved categories, with Class D being used for multicast and Class E being retained for use in the future.
3. In IPv4, the Host ID makes up the final second of Class A, B, and C, whereas the Network ID makes up the first half.
4. The Network ID always identifies the network in a certain location, but the Host ID always displays the number of hosts or nodes in a specific network.

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Fig 3.4 Different classes and their properties

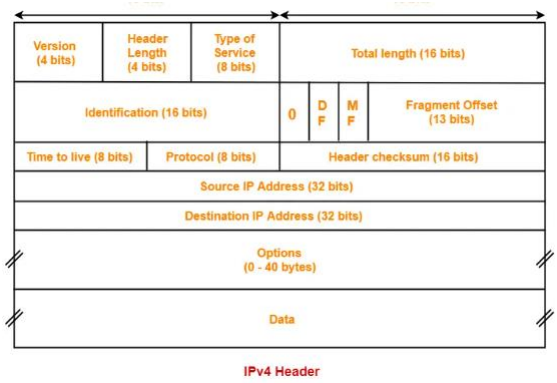

Fig 3.4.1 IPv4 Header

Let's walk through all these fields:

Version: the first field tells us which IP version we are using, only IPv4 uses this header so you will always find decimal value 4 here.

1. **Header Length**: this 4 bit field tells us the length of the IP header in 32 bit increments. The minimum length of an IP header is 20 bytes so with 32 bit increments, you would see value of 5 here. The maximum value we can create with 4 bits is 15 so with 32 bit increments, that would be a header length of 60 bytes. This field is also called the Internet Header Length (IHL).
2. **Type of Service**: this is used for QoS (Quality of Service). There are 8 bits that we can use to mark the packet which we can use to give the packet a certain treatment. You can read more about this field in my IP precedence and DSCP lesson.
3. **Total Length:** this 16-bit field indicates the entire size of the IP packet (header and data) in bytes. The minimum size is 20 bytes (if you have no data) and the maximum size is 65.535 bytes, that's the highest value you can create with 16 bits.
4. **Identification:** If the IP packet is fragmented then each fragmented packet will use the same 16 bit identification number to identify to which IP packet they belong to.
5. **IP Flags:** These 3 bits are used for fragmentation:
6. The first bit is always set to 0.
7. The second bit is called the DF (Don't Fragment) bit and indicates that this packet should not be fragmented.
8. The third bit is called the MF (More Fragments) bit and is set on all fragmented packets except the last one.
9. **Fragment Offset:** this 13 bit field specifies the position of the fragment in the original fragmented IP packet.

10. **Time to Live:** Everytime an IP packet passes through a router, the time to live field is decremented by 1. Once it hits 0 the router will drop the packet and sends an ICMP time exceeded message to the sender. The time to live field has 8 bits and is used to prevent packets from looping around forever (if you have a routing loop).
11. **Protocol:** this 8 bit field tells us which protocol is enapsulated in the IP packet, for example TCP has value 6 and UDP has value 17.
12. **Header Checksum:** this 16 bit field is used to store a checksum of the header. The receiver can use the checksum to check if there are any errors in the header.
13. **Source Address:** here you will find the 32 bit source IP address.
14. **Destination Address:** and here's the 32 bit destination IP address.
15. **IP Option:** this field is not used often, is optional and has a variable length based on the options that were used. When you use this field, the value in the header length field will increase. An example of a possible option is "source route" where the sender requests for a certain routing path.

Fragmentation

Fragmentation is the breaking of an IPV4 packet that exceeds the MTU of the data link layer into smaller IPV4 packets. Fragmentation is a process performed by the sender or the forwarding routers.

Fragmentation relies on some of the fields in the IPV4 header, which are as follows:

- ✓ **Identification:** To identify fragments, we use a 16-bit field. When the packet is fragmented, the identification field is copied into the fragmented packet headers to help determine that the packet belongs to a specific frame.
- ✓ **Fragment offset**: This is a 13-bit field that is used to order the data into fragments; it helps in the rearranging part. As discussed above, the largest data offset can be65,51565,515, but we need1616 bits to represent this number. The solution is to scale down by introducing a scaling factor. As we can see below, the scaling factor is equal to88. This means all the fragments except the last one should have data in multiples of8.

  $$\frac{2^{16}}{2^{13}} = 8$$

- ✓ **MF (More fragments):** It is a one-bit flag that specifies if there are more fragments of the frame. All the fragmented packets have this flag set to 11 except the last packet which sets this flag to 00. This flag along with the fragment offset helps the receiver identify the order during reassembly.
- ✓ **DF (Don't fragment):** It is a one-bit flag that tells the routers whether to fragment the packet or not. If it is set to 00 then the packet can be fragmented.

Reassembly

- ✓ The reassembly process is carried out at the destination. This is because packets take different routes through the network and arrive at different times.
- ✓ The steps of the process of reassembly are as follows:
- ✓ The destination identifies that the packet has been fragmented using the MF and fragment offset fields.
- ✓ The destination categorizes the incoming packets according to their identification fields. Two packets with the same identification field are put in the same category.
- ✓ The packets within a category are sequenced using the MF and fragment offset. First, the packets with MF equal to 11 are sorted in ascending order based on their fragment offset values. Then the packet having an MF equal to 00 and a fragment offset not equal to 0 is placed at the end, since it's the last packet.

Switching Modes

1. The layer 2 switches are used for transmitting the data on the data link layer, and it also performs error checking on transmitted and received frames.
2. The layer 2 switches forward the packets with the help of MAC address.
3. Different modes are used for forwarding the packets known as **Switching modes**.
4. In **switching mode**, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.

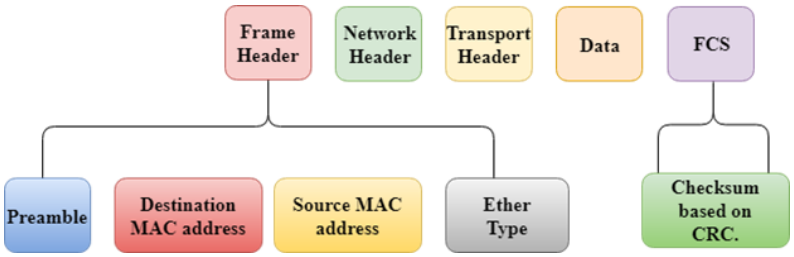

Fig 3.5 Frame of switching mode

There are three types of switching modes:

1. Store-and-forward
2. Cut-through
3. Fragment-free

Store-and-forward

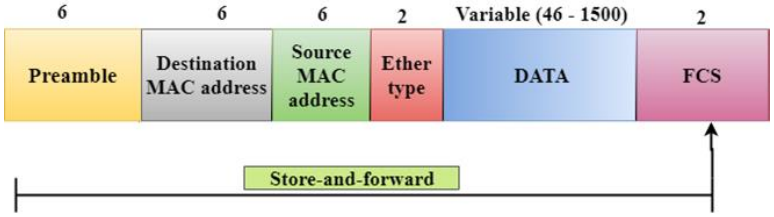

Fig 3.6 Stop and forward frame

- ✓ Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- ✓ The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as storing the frame.
- ✓ When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as forwarding the frame.
- ✓ CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- ✓ The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- ✓ Store-and-forward switches are highly reliable as it does not forward the collided frames.

Cut-through Switching

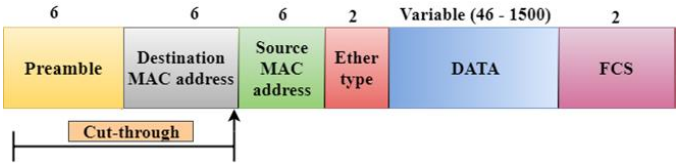

Fig 3.7 Cut-Through Switching

- ✓ Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- ✓ Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- ✓ It has low latency rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- ✓ It has no error checking technique. Therefore, the errors can be sent with or without errors to the receiver.
- ✓ A Cut-through switching technique has low wait time as it forwards the packets as soon as it identifies the destination MAC address.
- ✓ In this technique, collision is not detected, if frames have collided will also be forwarded.

Fragment-free Switching

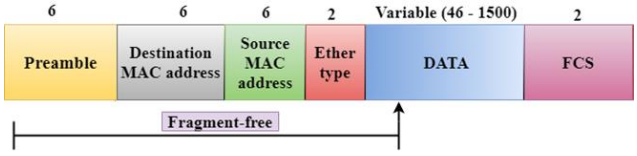

Fig 3.8 Fragment-Free Switch

- ✓ A Fragment-free switching is an advanced technique of the Cut-through Switching.
- ✓ A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- ✓ It combines the speed of Cut-through Switching with the error checking functionality.
- ✓ This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- ✓ A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Differences b/w Store-and-forward and Cut-through Switching.

Store-and-forward Switching	Cut-through Switching
Store-and-forward Switching is a technique that waits until the entire frame is received.	Cut-through Switching is a technique that checks the first 6 bytes following the preamble to identify the destination address.
It performs error checking functionality. If any error is found in the frame, the frame will be discarded otherwise forwarded to the next node.	It does not perform any error checking. The frame with or without errors will be forwarded.
It has high latency rate as it waits for the entire frame to be received before forwarding to the next node.	It has low latency rate as it checks only six bytes of the frame to determine the destination address.
It is highly reliable as it forwards only error-free packets.	It is less reliable as compared to Store-and-forward technique as it forwards error prone packets as well.
It has a high wait time as it waits for the entire frame to be received before taking any forwarding decisions.	It has low wait time as cut-through switches do not store the whole frame or packets.

Table 3.0 Difference between Store and forward switching and cut through switching

Routing in a Datagram Network

The diagram below shows a message being send by host H1 to host H2. The Internet Service Provider (ISP) comprises of five routers that are numbered from 1 to 5. H1 is connected to router 1 while H2 is connected to router 5.
Suppose that the message is of such a size that it has to be broken into 4 packets. The packets are labelled as A, B, C and D.
Each of the five routers maintains a routing table that has two columns, DEST storing the destination node and NEXT storing next node. To reach the DEST node the packet is routed via the NEXT node. The routing tables are dynamic in nature that are refreshed time to time depending upon the network conditions.

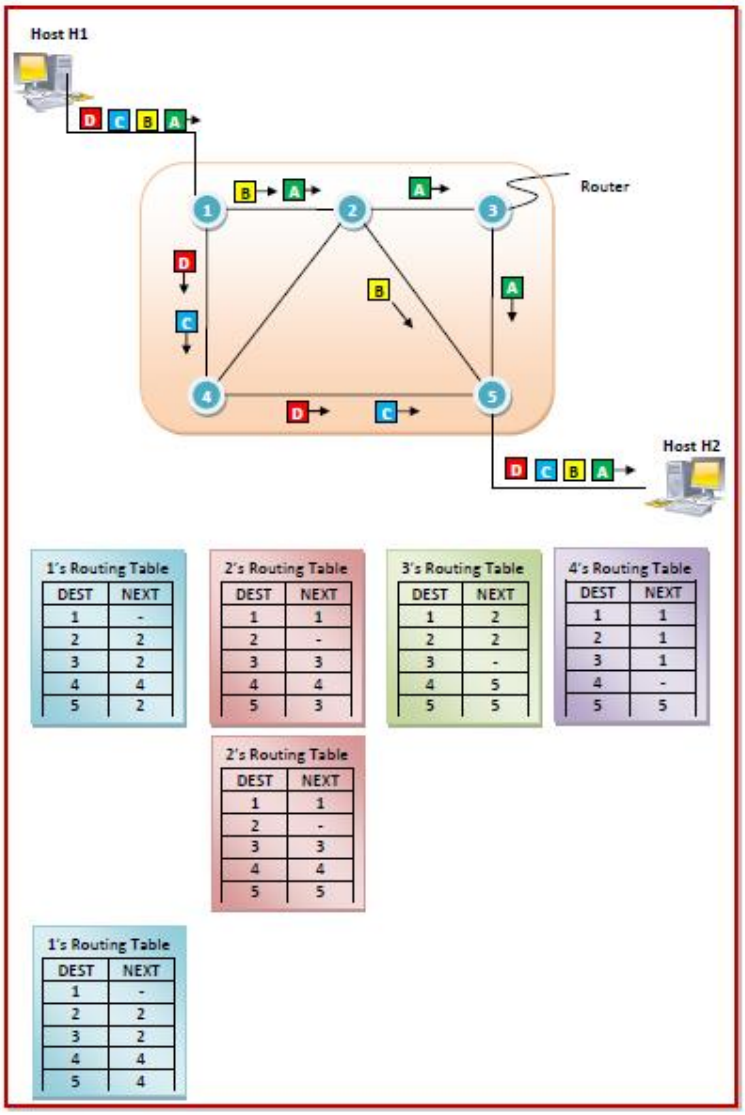

Fig 3.9 Illustrate of Routing within a datagram network

When packet A is to be transmitted, it is transferred to router 1 by host H1. The destination is router 5, since host H2 is connected to it. Router 1 consults its routing table (the one in the top row) and sends the packet to router 2. Router 2 sends it to router 3 which sends it to router 5.
So, the path of packet A is 1 − 2 − 3 − 5.
When packet B is to be transmitted, the routing table of router 2 has changed. Consequently, the path of packet B is different from that of A.

The path of packet B is 1 − 2 − 5.
When packet C is to be transmitted, the routing table of router 1 has changed.
Thus, the path of packet C is 1 − 4 − 5.
The routing tables remain same for the next packet. So, the path doesn't change for it.
Hence, the path of packet D is again 1 − 4 − 5.

Routing by a Virtual-Circuit Network

In the adjoining diagram, we can see that the Internet Service Provider (ISP) has six routers (1 to 6) connected by transmission lines shown in black lines. There are three hosts, host H1 and H3 are connected to router 1, while host H2 is connected to router 6.
Suppose that hosts H1 and H3 both wants to send data packets to host H2. Virtual circuits are established between the hosts to enable data transmission. For H1, a virtual circuit via the routers 1 – 2 – 6 is established, as denoted by green dotted lines. All its packets, 1A, 1B, 1C and 1D are routed through this circuit. In the same way, another virtual circuit via the routers 1 – 2 – 3 – 6 is established, as denoted by red dotted lines. H3's packets 3A, 3B and 3C are routed through this circuit. Each router maintains a separate entry in the routing table for each virtual circuit that it is a part of.

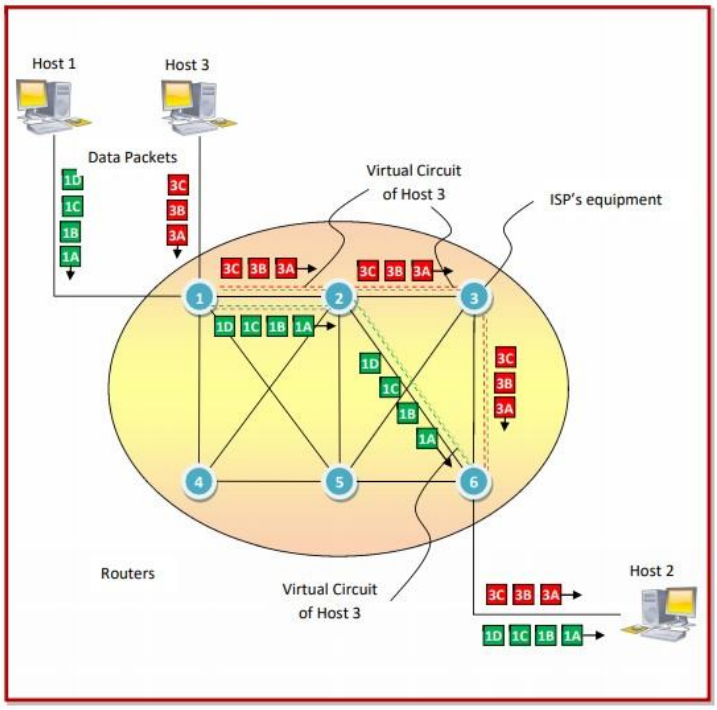

Fig 3.10 Illustrate of Routing within a Virtual circuit network

Routing algorithm

1. In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
2. Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
3. The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
4. Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

1. Adaptive Routing algorithm
2. Non-adaptive Routing algorithm

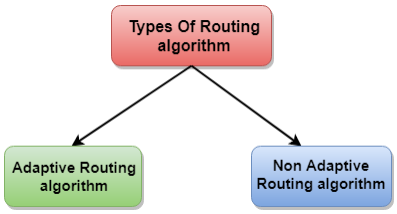

Fig 3.11 types of routing algorithm

Adaptive Routing algorithm

1. An adaptive routing algorithm is also known as dynamic routing algorithm.
2. This algorithm makes the routing decisions based on the topology and network traffic.
3. The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

1. **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation.
2. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
3. **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
4. **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

1. Non Adaptive routing algorithm is also known as a static routing algorithm.
2. When booting up the network, the routing information stores to the routers.
3. Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

1. **Flooding:** In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.
2. **Random walks:** In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

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

Table 3.4 Adaptive and Non-Adaptive Routing Algorithm

Traffic-aware routing in computer networks

Traffic awareness is one of the approaches for congestion control over the network. The basic way to avoid congestion is to build a network that is well matched to the traffic that it carries. If more traffic is directed but a low-bandwidth link is available, congestion occurs.
The main goal of traffic aware routing is to identify the best routes by considering the load, set the link weight to be a function of fixed link bandwidth and propagation delay and the variable measured load or average queuing delay. Least-weight paths will then favour paths that are more lightly loaded, remaining all are equal.
The traffic aware routing is diagrammatically represented as follows −

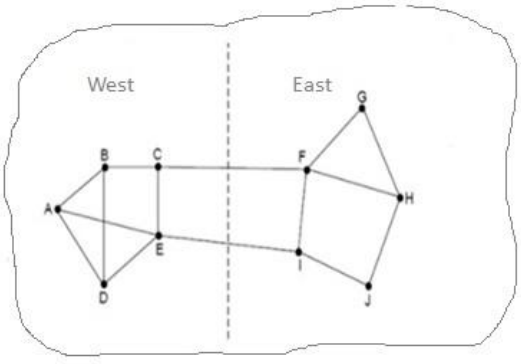

Fig 3.12 Traffic-aware routing in computer networks

Explanation

Step 1 − Consider a network which is divided into two parts, East and West both are connected by links CF and EI.
Step 2 − Suppose most of the traffic in between East and West is using link CF, and as a result CF link is heavily loaded with long delays. Including queueing delay in the weight which is used for shortest path calculation will make EI more attractive.

Step 3 − After installing the new routing tables, most of East-West traffic will now go over the EI link. As a result in the next update CF link will appear to be the shortest path.
Step 4 − As a result the routing tables may oscillate widely, leading to erratic routing and many potential problems.
Step 5 − If we consider only bandwidth and propagation delay by ignoring the load, this problem does not occur. Attempts to include load but change the weights within routing scheme to shift traffic across routes arrow range only to slow down routing oscillations.
Step 6 − Two techniques can contribute for successful solution, which are as follows −

1. Multipath routing
2. The routing scheme to shift traffic across routes.

Features

The features of traffic-aware routing are as follows −

- ✓ It is one of the congestion control techniques.
- ✓ To utilise most existing network capacity, routers can be tailored to traffic patterns making them active during daytime when network users are using more and sleep in different time zones.
- ✓ Roots can be changed to shift traffic away because of heavily used paths.
- ✓ Network Traffic can be split across multiple paths.

Random Early Detection (RED)

Random Early Detection (RED) is a congestion control algorithm used in computer networking to manage and prevent congestion in network routers. It is primarily employed in IP (Internet Protocol) networks, especially within the TCP/IP suite. RED aims to avoid network congestion by dropping or marking packets before the network becomes severely congested. Here's an overview of how RED works and its key principles:

Working Principles of RED:
1. Queue Management:
- RED operates at the router's queue level, specifically in the output queues where packets wait to be transmitted.
- Each queue in a router has a configurable minimum and maximum threshold for the number of packets it can hold.

2. Marking and Dropping Packets:
- When the average queue size is below the minimum threshold, all incoming packets are accepted without any drop or marking.
- When the queue size exceeds the maximum threshold, RED starts to take action.
- RED probabilistically marks or drops packets rather than taking a deterministic approach. This means that packets are randomly selected for marking or dropping, based on a set of parameters.

3. Packet Selection for Marking/Dropping:
- RED calculates a measure called the "average queue size" (usually an exponentially weighted moving average) to assess the congestion level.
- Incoming packets are evaluated against the average queue size.
- The probability of marking or dropping a packet depends on this average queue size.
- The higher the average queue size relative to the maximum threshold, the higher the probability of a packet being marked or dropped.

4. Traffic Control:
- RED provides feedback to TCP flows by marking packets with Explicit Congestion Notification (ECN) bits set in the packet header. This informs the sender that network congestion might be occurring.

- RED also drops packets as a last resort when the queue size exceeds a pre-defined hard limit, preventing excessive queue buildup.

Advantages of RED:

- Early Congestion Detection: RED detects congestion before it reaches a critical level, preventing network performance degradation and packet loss.
- Fairness: RED promotes fairness among TCP flows, as it marks and drops packets probabilistically rather than treating all flows equally.
- Improved Utilization: It helps in the efficient utilization of network resources by avoiding unnecessary overloads.

Challenges and Configuration:

- Configuring RED requires careful parameter tuning to ensure it behaves optimally for a specific network environment.
- Setting the minimum and maximum thresholds, as well as the parameters that control the marking/dropping probability, is essential to achieving desired performance.

Explicit Congestion Notification (ECN)

Explicit Congestion Notification (ECN) is a congestion control mechanism used in computer networks, primarily within the Transmission Control Protocol (TCP) and Internet Protocol (IP) suite. ECN allows routers and network devices to signal congestion to endpoints (senders and receivers) explicitly rather than relying solely on packet loss as an indicator of congestion. This mechanism helps improve network efficiency and performance while reducing the occurrence of packet loss. Here are the key aspects of ECN:

How ECN Works:

1. ECN-Capable Devices: Both the sending and receiving devices in a communication session need to be ECN-capable. They signal their support for ECN during the initial handshake.

2. ECN Field in IP Header: ECN is implemented by adding two bits, ECN-Capable Transport (ECT) and ECN Congestion Experienced (CE), to the IP header. These bits are used to mark packets as they traverse the network.

3. Router Marking: Routers in the network monitor their congestion levels. When a router experiences congestion but doesn't drop packets immediately, it marks the packets with the CE (Congestion Experienced) bit set in the IP header. This indicates that the network is becoming congested.

4. Forwarding ECN Markings: Routers along the packet's path continue to forward the ECN markings. If a router receives a packet marked as ECN-capable (ECT = 1) and experiences congestion, it marks the packet with CE = 1 and forwards it.

5. Receiver's Feedback: The receiving end, upon receiving an ECN-marked packet, does not drop the packet but may use this information to provide feedback to the sender about network congestion. This feedback can be communicated through TCP acknowledgments.

6. Sender's Reaction: The sender, upon receiving an acknowledgment with the ECN Echo (ECE) bit set, knows that congestion is occurring in the network. It reacts to this feedback by reducing its transmission rate, similar to how it would respond to packet loss.

7. Fallback to Packet Loss: ECN is designed to complement, not replace, packet loss as an indicator of congestion. If ECN is not effectively supported or utilized, traditional packet loss-based congestion control mechanisms still come into play.

Advantages of ECN:

- Reduced Packet Loss: ECN helps reduce the occurrence of packet loss during congestion, improving network efficiency and application performance, especially for real-time applications.

- Better Network Utilization: ECN enables more proactive congestion control, allowing the network to operate closer to its capacity without unnecessary packet drops.

- Improved User Experience: Applications and users experience fewer retransmissions and smoother network performance.

Challenges and Considerations:

- ECN requires support from both network infrastructure and end systems.

- Some older network devices and routers may not support ECN, which can limit its effectiveness.

- Proper configuration and monitoring are necessary to ensure that ECN operates as intended and does not lead to unintended side effects.

Classless Inter-Domain Routing

CIDR, or Classless Inter-Domain Routing, is a method of IP address allocation and route aggregation that helps reduce the size of routing tables in the Internet's global routing system. It replaces the traditional class-based IP address scheme with a more flexible and efficient approach. CIDR notation represents IP addresses and their associated network prefixes in a concise and hierarchical manner. Here's an explanation of CIDR with an example:

CIDR Notation:

CIDR notation uses a combination of an IP address and a prefix length, separated by a forward slash ("/"). The IP address represents the network's base address, and the prefix length indicates the number of bits set to 1 in the network's subnet mask. The prefix length effectively defines the size of the network.

The format is as follows: `IP_address/prefix_length`.

Example:

Let's consider an example using CIDR notation:

Suppose an organization is allocated the IP address block `192.168.1.0/24`.

- `192.168.1.0` is the base IP address.

- `/24` indicates that the first 24 bits (the leftmost portion) are part of the network address, and the remaining 8 bits (the rightmost portion) are available for host addresses within the network.

To understand the subnet mask:

- A subnet mask of `255.255.255.0` in dotted-decimal notation corresponds to `/24` in CIDR notation.

- In binary, the subnet mask is `11111111.11111111.11111111.00000000`, where the first 24 bits are set to 1, and the last 8 bits are set to 0.

Now, let's break down the CIDR notation for this example:

- IP Address: `192.168.1.0`

- Prefix Length: `/24`

This means that the organization has been assigned the IP address range from `192.168.1.0` to `192.168.1.255`. Within this range, there are 256 unique host addresses (from 0 to 255).

CIDR allows for a high degree of flexibility. For instance:

- You can use a shorter prefix length (e.g., `/25`) to create two smaller subnets with 128 host addresses each.

- You can use a longer prefix length (e.g., `/23`) to combine multiple contiguous subnets into a larger one.

CIDR notation is crucial for efficient IP address allocation and routing table management in modern networking, as it enables the aggregation of routes and reduces the size of routing tables, leading to more efficient use of IP address space and improved Internet routing performance.