3.Network Layer

The network layer is primarily responsible for facilitating the transmission of packets from the source node to the destination node. In order to do this, it is important for the network layer to possess knowledge on the network's topology, encompassing all routers and links. Subsequently, the network layer may make informed decisions in selecting suitable pathways inside the network. It is important to use caution in the selection of routes to prevent the excessive burdening of some communication lines and routers, while leaving others underutilised.When the source and destination are located on separate networks, additional challenges arise. The responsibility for addressing and managing these issues lies at the network layer.The primary duty is delivering services to the transport layer. It is essential that the provision of services be detached from the underlying router technology.It is essential to ensure that the transport layer remains isolated from any knowledge pertaining to the number, categorization, and arrangement of routers inside the network infrastructure.

Store and forward packet switching:

The equipment of the ISP (routers linked by transmission lines), depicted within the shaded oval, and the equipment of the customers, illustrated outside the oval, constitute the primary constituents of the network.Connected directly to one of the ISP's routers, A, Host H1 may be a personal computer with a DSL modem inserted in.H2 is connected to a LAN, which may be an office Ethernet, via a customer-owned and operated router, F.F has been positioned outside the oval in this context due to its non-belonging status to the ISP.

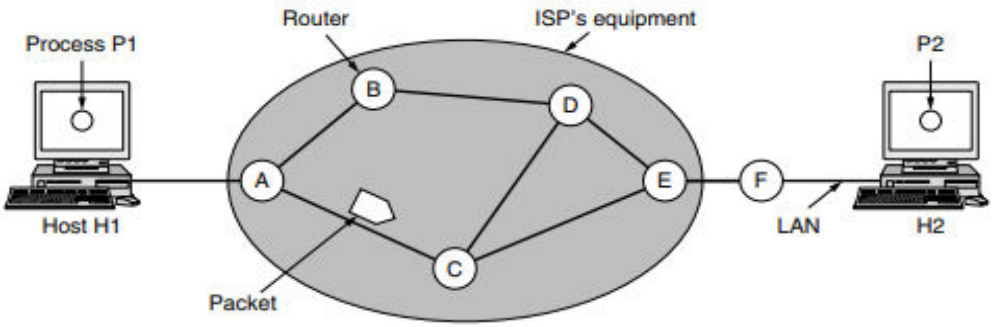


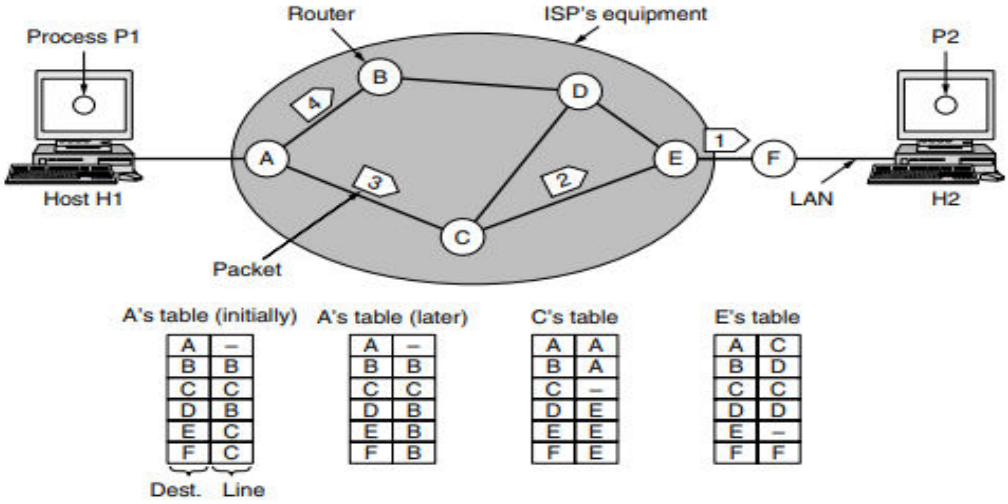
Figure 5-1. The environment of the network layer protocols.

When a host has a packet to transmit, it does so via a point-to-point link to the ISP or its own LAN to the nearest router. The packet remains in that location until it has completely arrived and the link has completed its processing, which includes checksum verification. It is then transmitted to the subsequent router along the path until it arrives at the destination host, where it is unpacked. This is store-and-forward packet switching in action.

Implementation of Connectionless Service:

In the event that CL service is provided, packets are independently injected into the network and subsequently routed. No setup in advance is required. The network is referred to as a datagram network, and the packets are often referred to as datagrams.

When connection-oriented service is implemented, prior to transmitting data packets, a path must be established from the source router to the destination router. Comparable to the physical circuits established by the telephone system, this connection is referred to as a VC (virtual circuit), and the network is known as a virtual-circuit network. Internal tables within every router specify where to forward packets. Every entry in the table comprises a dyad, which includes a destination and the corresponding outgoing line. Only lines with direct connections are permitted. Since A possesses solely two outgoing lines, which are directed to B and C, any incoming packet must be routed through one of these routers, notwithstanding its ultimate destination being another router. The figure displays the initial routing table for A, denoted by the label "initially."

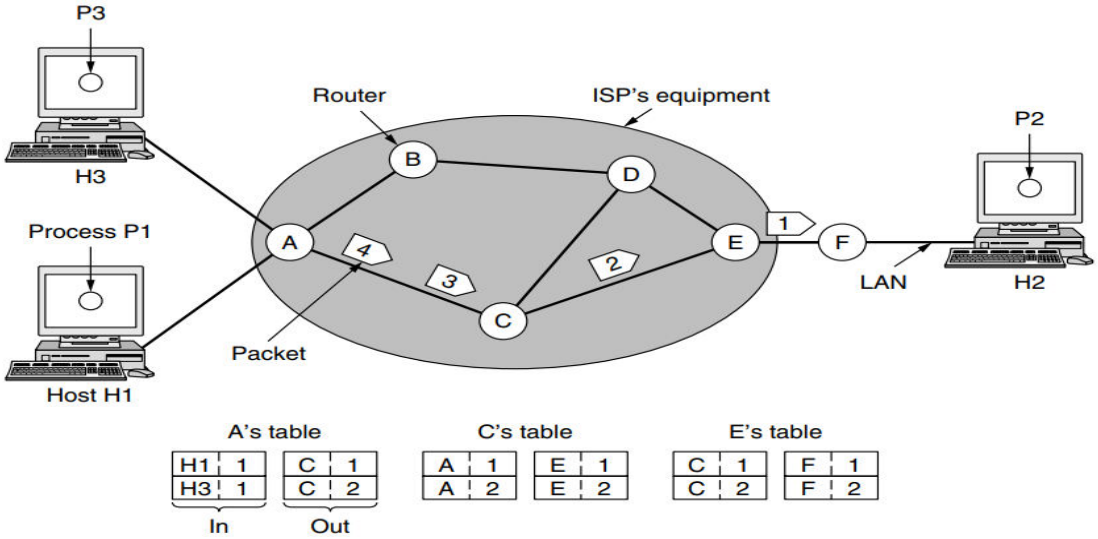


At location A, packets 1, 2, and 3 are temporarily held after being received over the incoming connection and undergoing checksum verification then, every packet is routed in accordance with the routing table of node A, and then sent across the outgoing connection leading to node C.

However, packet 4 experiences a distinct occurrence. Upon reaching point A, the data is sent to router B, despite its intended destination being F. Due to an unidentified reasoning, A opted to transmit packet 4 via an alternative route in contrast to the preceding three packets. It is possible that the system has acquired information on a congestion event along the ACE route and subsequently modified its routing table, as seen in the section labelled "later." The algorithm responsible for managing the tables and determining the routing choices is sometimes referred to as the routing algorithm. For connection-oriented connections, a virtual circuit network is required.

As part of the connection configuration, a route from the source machine to the destination machine is selected and stored in routing tables when the connection is established. This path is utilised by all traffic

traversing the connection. Upon the discharge of the connection, the virtual circuit is likewise terminated. In connection-oriented service, a unique identifier is appended to each transmission, specifying to which virtual circuit it is associated. Host H1 and host H2 have established connection 1.According to the first line of A's table, in the event that a transmission arrives from H1 with the connection identifier 1, it is to be forwarded to router C with the same connection identifier 1.In a similar fashion, the initial entry at C assigns connection identifier 1 to the transmission and forwards it to E.



If H3 desires to establish a connection with H2, it will select connection identifier 1 and instruct the network to establish the virtual circuit. Consequently, the second row in the tables is generated. While A can readily differentiate between connection 1 packets originating from H1 and those from H3, C lacks this capability. Consequently, A assigns a distinct connection identifier to the outgoing traffic for the second connection.

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

Routing Algorithms

The routing algorithm is a crucial component of the network layer software, since it is tasked with determining the appropriate output line for transmitting incoming packets. Once a prominent broadcasting network is established, it is often anticipated to operate consistently over an extended period of time, devoid of any significant disruptions or malfunctions.

During that time frame, several types of hardware and software problems are expected to occur. The occurrence of failures in hosts, routers, and lines will be frequent, leading to many changes in the network architecture. The routing algorithm must possess the capability to effectively handle variations in both the network architecture and traffic conditions. Routing algorithms may be categorised into two primary classes: nonadaptive and adaptive. Nonadaptive algorithms make routing choices without considering any measurements or estimations of the existing topology and traffic. The selection of the route is precalculated. This particular process is sometimes referred to as static routing.

In contrast, adaptive algorithms modify their routing choices in response to changes in the topology and traffic conditions. The information used by these dynamic routing techniques is obtained from neighbouring routers. The metrics used for optimisation include distance, the number of hops, and travel time.

Shortest Path Algorithm

The proposed concept involves constructing a graphical representation of the network, whereby individual nodes within the graph symbolise routers, and the edges within the graph symbolise communication lines.In order to determine the optimal path between two designated routers, the method simply identifies the shortest route connecting them inside the graph.

The computation of edge labels may be determined using a function that takes into account many aspects such as distance, bandwidth, average traffic, communication cost, observed latency, and other relevant considerations.

The distance from the source node along the best known route is denoted by a label in brackets for each node. At beginning, the absence of any known pathways necessitates the assignment of an infinite label to all nodes. As the algorithm progresses and discovers pathways, the labels have the potential to undergo modifications, indicating the presence of improved paths.A designation may be categorised as either provisional or enduring. At the beginning, it is important to note that all labels are subject to revision and should be considered provisional. Once the shortest feasible route from the source to a particular node is determined, it is permanently established and remains unchanged afterward.

Determine the shortest distance between points A and D. We commence by designating node A as permanent, denoted by a circle that is entirely filled in.Examine and relabel each of the adjacent nodes to A (the working node) with its distance to A.

1. Make the router, which is a local node, the tree's root. This node should have a cost of 0 and be the first fixed node.

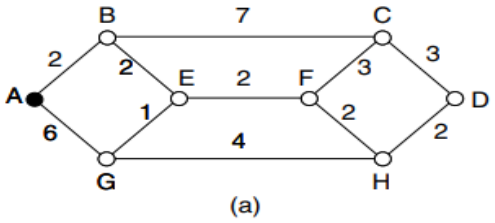
2. Look at every node that is close to the last fixed node.

3. Assign each node a total cost and make it an estimate.

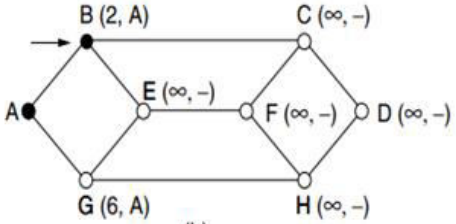
4. From the list of possible nodes, a. Pick the one with the lowest cost and make it permanent.

b. If there are more than one way to get to a point, choose the one with the lowest total cost.

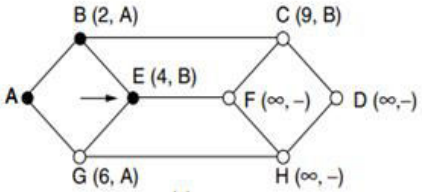
5. Do steps 2 through 4 again and again until every node is fixed.



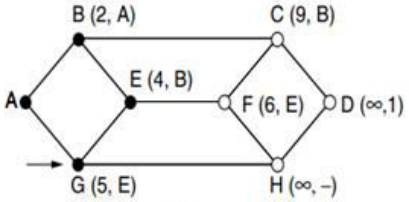
(a)



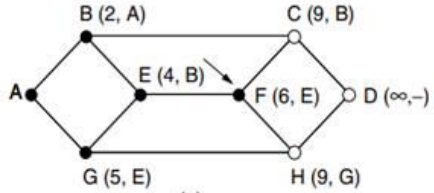
(b)



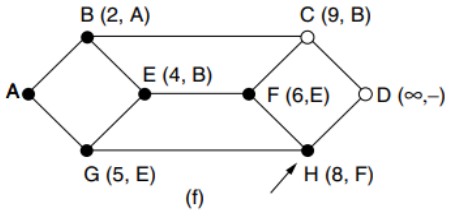
(c)



(d)



(e)



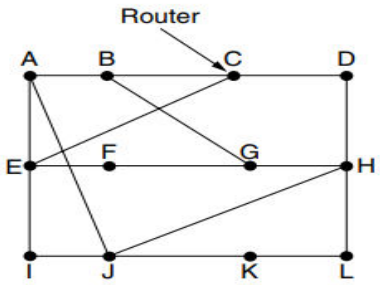
(f)

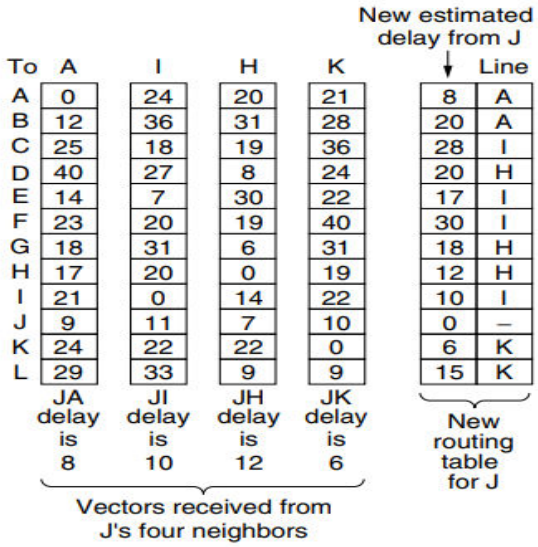
Flooding

One often used method is known as flooding, when each incoming packet is sent via every outgoing line, with the exception of the line through which it was received.Flooding, a well-known phenomenon in network communication, results in the generation of a significant volume of duplicate packets. In response to this issue, many solutions have been implemented to effectively manage and regulate the flooding process.One potential approach for attaining this objective is the implementation of a mechanism whereby the router assigns a unique sequence number to every packet it receives from the connected hosts.This algorithm is strong and resilient. As long as a sufficient number of routers are not working properly, packets can still get to where they are supposed to go.

Distance Vector Routing

Two widely used dynamic methods in computer networking are distance vector routing and link state routing. Every router maintains a database, often referred to as a vector, that contains information on the optimal distance to each destination and the corresponding link that should be used to reach that destination. The tables undergo updates via the exchange of information with neighbouring entities. Over time, each router acquires knowledge about the optimal connection to establish connectivity with every destination.The routing method known as the distance vector algorithm is often referred to as the Bellman-Ford routing algorithm.



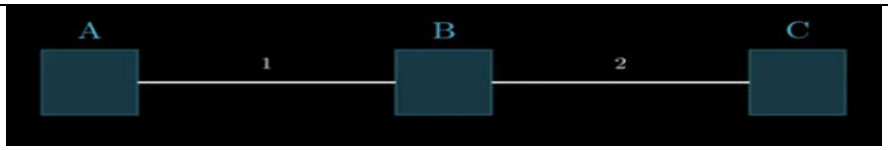


Let us examine the process by which J determines its updated path to router G. It is aware that it can reach destination A within a time frame of 8 milliseconds. Additionally, destination A claims that it can reach destination G within a time frame of 18 milliseconds. Consequently, destination J is aware that it can rely on a delay of 26 milliseconds to reach destination G if it passes packets intended for G to destination A. In a similar manner, the computation of the delay from G to I, H, and K is as follows: 41 milliseconds (31 milliseconds + 10 milliseconds), 18 milliseconds (6 milliseconds + 12 milliseconds), and 37 milliseconds (31 milliseconds + 6 milliseconds), respectively.

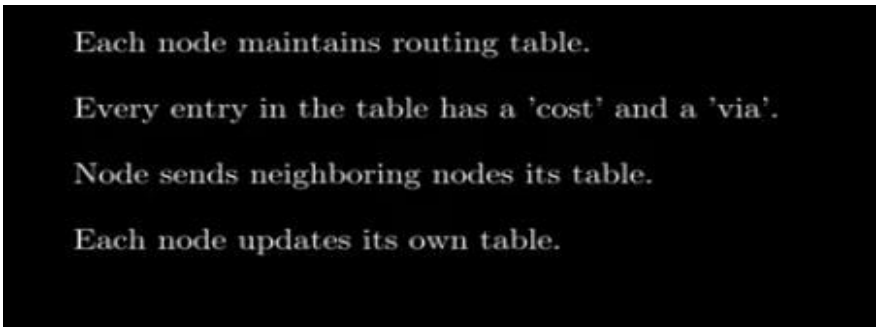
The optimal value among the given options is 18, thereby causing the system to record an entry in its routing database indicating that the delay to destination G is 18 milliseconds and the recommended route is via node H. The same computation is executed for each of the other destinations, resulting in the updated routing table shown in the last column of the diagram.

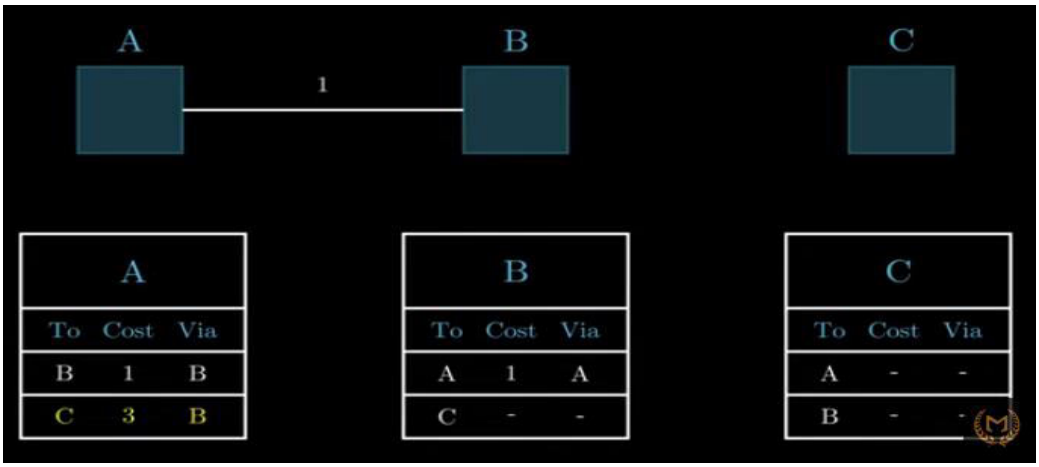
Count to Infinity Problem:

The issue arises when the nodes inside the network use the Distance Vector Routing (DVR) Protocol.



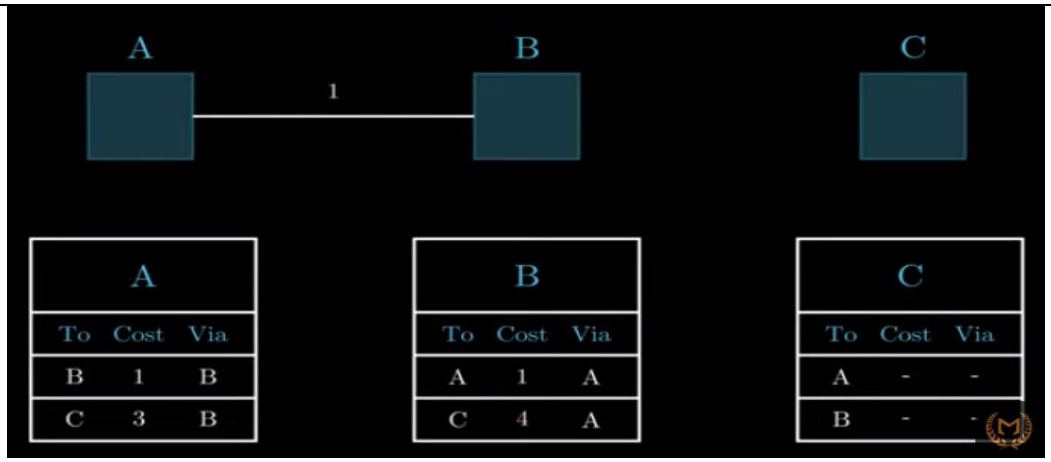
Router A will infer that it has the capability to establish a connection with Router B with a cost of 1 unit, whereas Router B will infer that it has the capability to establish a connection with Router C with a cost of 2 units.





The scenario shown in the previous image involves the disconnection of the connection between points B and C. In this scenario, B will get the knowledge that it is no longer feasible to reach C with a cost of 2, and then modify its table to reflect this change.

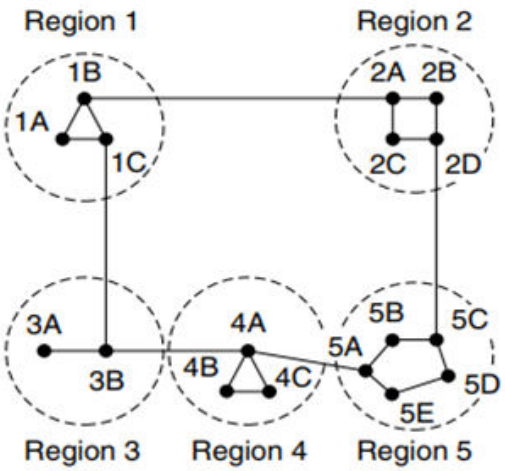
Nevertheless, it is possible that A transmits some data to B indicating the feasibility of establishing a connection between A and C, although at a cost of 3. Subsequently, given that B can establish a connection with A at a cost of 1, B will mistakenly revise its table to reflect that it can establish a connection with C via A at a cumulative cost of 1 + 3 = 4 units.



Subsequently, A will get notifications from B and proceed to adjust its expenses to a value of 4, and this process will continue iteratively. Consequently, the system becomes trapped in a cycle of negative feedback, resulting in an exponential increase in costs. The phenomenon at hand is often referred to as the Count to Infinity issue.

Hierarchical routing

As the size of networks increases, the routing tables of routers also increase in proportion.The use of router memory is not only related to the continuous growth of tables, but also necessitates more CPU time for scanning and increased bandwidth for transmitting status reports.At a certain point, the network may expand to a magnitude where it becomes impractical for each router to possess an entry for every other router. Consequently, routing will need to be executed in a hierarchical manner, akin to the telephone network.In the context of network routing, the implementation of hierarchical routing involves the partitioning of routers into distinct zones.



Full table for 1A

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

Hierarchical table for 1A

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

Every router has a thorough understanding of the routing of packets to destinations inside its own region, while remaining unaware of the internal architecture of other regions.In the case of large networks, a two-tiered structure may become inadequate, hence necessitating a division of regions into clusters, clusters

into zones, zones into groups, and so on. Router 1A has a complete routing table including a total of 17 entries. In the hierarchical routing approach, local routers are assigned individual entries, while all other regions are consolidated into a singular router. Consequently, traffic destined for region 2 is directed over the 1B-2A line, while the other traffic is routed via the 1C-3B line. The implementation of hierarchical routing has resulted in a decrease in the number of entries in the table, namely from 17 to 7.

There exists a consequence that must be paid, namely a slight increase in the length of the route. since an example, the optimal path from location 1A to location 5C is found by traversing region 2. However, in the context of hierarchical routing, all traffic destined for region 5 is directed via region 3, since this routing strategy proves more advantageous for the majority of destinations inside region 5.When confronted with the scenario of a much expanded network, a pertinent inquiry arises: "What is the optimal number of levels for the hierarchy?" As an example, let us suppose a network with 720 routers. In the absence of a hierarchical structure, it is necessary for each router to possess a total of 720 routing table entries.

In the scenario where the network is divided into 24 regions, with each region consisting of 30 routers, it is necessary for each router to maintain 30 local entries and 23 distant entries, resulting in a cumulative total of 53 entries.In the case of choosing a three-level hierarchy, in which there are 8 clusters, each including 9 regions consisting of 10 routers, it is necessary for each router to possess 10 entries for local routers, 8 entries for routing to other regions within its own cluster, and 7 entries for distant clusters. Consequently, the total number of entries required per router amounts to 25.

Link State Routing

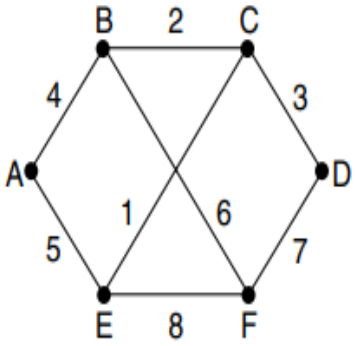
The main issue observed in DVR was the prolonged convergence time in the network architecture, due to the count-to-infinity problem. As a result, it was subsequently replaced by a completely novel method known as link state routing. The concept behind link state routing is quite straightforward and can be delineated into five components. Every router is required to perform the following tasks:

Explore the adjacent entities and get knowledge about their network addresses. Assign a distance or cost measure to each of its neighbouring entities. Compose a comprehensive document encapsulating the whole of the acquired knowledge. Transmit this data packet to and establish communication with all other routers in the network. Calculate the most efficient route to each additional router. The whole architecture is effectively disseminated to each individual router.

Subsequently, the use of Dijkstra's algorithm may be employed at each router in order to determine the most optimal route to every other router inside the network.After booting, a router starts the process of identifying and acquiring information about its neighbouring routers. This objective is achieved by transmitting a distinct HELLO packet over each individual point-to-point connection.It is anticipated that the router situated at the other end will transmit a response with its distinct identifier.The link state routing technique requires the presence of a distance metric for each connection in order to determine the shortest

pathways. The measurement of link delays may be regarded as a metric in some cases. The most straightforward method for determining this delay involves transmitting a specialised ECHO packet across the communication connection, which prompts the recipient to promptly return it.

By measuring the time it takes for a signal to travel from the sending router to the receiving router and back, and then dividing this value by two, the sending router may get a reasonably accurate approximation of the delay. Every router constructs a packet that includes all of the data.The packet starts with the sender's identification, which is thereafter accompanied by a sequence number and age, as well as a list of neighbouring entities. The cost assigned to each neighbour is also provided.



(a)

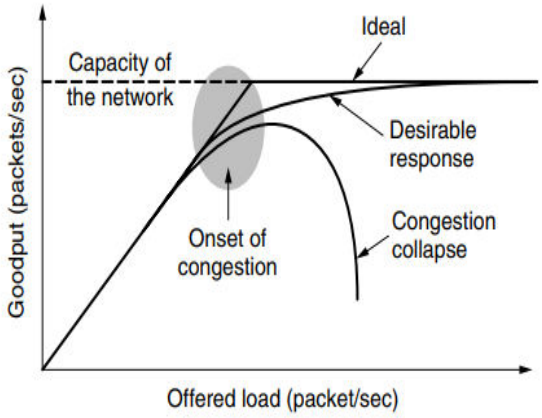
Link		State		Packets	
A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(b)

The distribution of link status packets to all routers may be achieved via the use of flooding. To regulate the flood, each packet is equipped with a sequence number that is increased for every new packet sent. In the event that a packet is fresh, it is forwarded over all lines except the one it was received on. Conversely, if a packet is identified as a duplicate, it is disregarded and not further processed.The distribution of link status packets to all routers may be achieved via the use of flooding. In this approach, each packet is equipped with a sequence number that is incremented for every new packet sent. To regulate the flood, the packet is forwarded over all lines, except the one it was received on, if it is determined to be fresh. Conversely, if the packet is identified as a duplicate, it is rejected.

Congestion Control

The presence of an excessive number of packets inside the network results in delays and losses of packets, hence leading to degradation in performance. The present circumstance might be referred to as congestion.The duty for managing congestion is shared between the network and transport levels.When hosts transmit packets into the network at a rate that is much below its maximum capacity, the quantity of packets successfully delivered is directly proportional to the quantity of packets transmitted.As the load being imposed on the system approaches its carrying capacity, intermittent traffic bursts result in the saturation of buffers inside routers, leading to occasional packet loss.

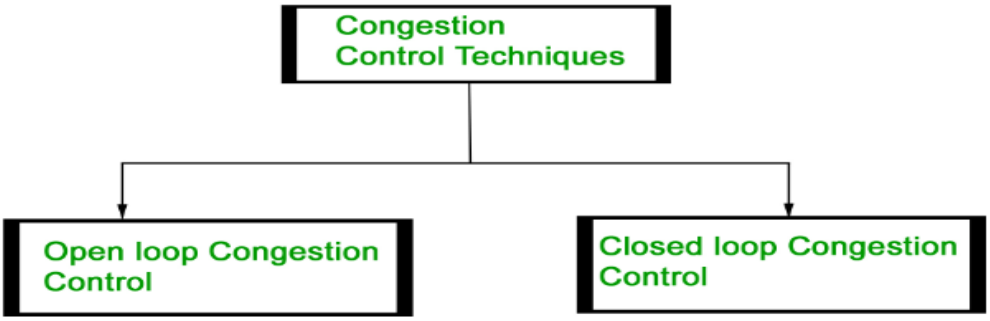


In the event that several streams of packets abruptly begin arriving on three or four input lines, all necessitating the same output line, a queue will accumulate. In the event that the available memory is inadequate to accommodate the whole of the packets, loss of packets will occur. The potential benefits of increasing memory capacity in routers are limited, since excessive memory allocation might exacerbate congestion issues rather than alleviate them. This phenomenon occurs due to the fact that packets, upon reaching the forefront of the queue, have already experienced many instances of timing out and subsequent transmission of duplicate packets. This exacerbates the situation, rather than improving it, since it contributes to congestion breakdown. Congestion may also occur in low-bandwidth lines or routers that exhibit slower packet processing rates compared to the line rate.

Congestion Control approaches

The existence of congestion indicates that the magnitude of the load exceeds the capacity of the available resources. Two potential approaches might be considered: increasing the available resources or reducing the current load.One fundamental approach to minimising congestion is the construction of a network that is appropriately designed to accommodate the volume of traffic it handles.In instances of significant congestion, resources have the potential to be included in a dynamic manner. This may be achieved via many means, such as activating additional routers that are available as backups or procuring more bandwidth from the open market. The process being referred to is often known as provisioning. Routes may be customised to accommodate fluctuations in traffic patterns that occur during the day, when network users residing in various time zones awaken and retire. The term used to describe this concept is traffic-aware routing.Occasionally, it may be unfeasible to increase the capacity. The only method to alleviate congestion is by reducing the overall burden.

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



Open loop congestion management rules are used as a proactive measure to mitigate congestion before it occurs. Congestion control is managed by either the source or the destination.The policies implemented by **open loop congestion management mechanisms are as follows:**

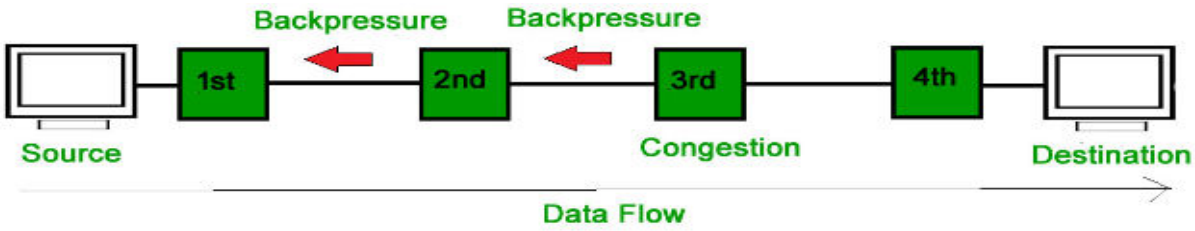
The retransmission policy refers to a set of guidelines or rules that govern the process of resending or retransmitting data packets in a communication system.

In the event that the sender perceives a loss or corruption of a sent packet, it becomes necessary to initiate the process of retransmission for such packet. The transmission has the potential to worsen network congestion. In order to mitigate congestion, it is essential to design transmission times that not only avoid congestion but also optimise efficiency. Congestion may also be impacted by the kind of window used at the sender's end. While some packets may be successfully received at the recipient end, many of the packets in the Go-back-n window are resent. This duplication can worsen and intensify the network's congestion. Selective repeat window should thus be used because it transmits the particular packet that could have been missed.One effective strategy used by routers is the implementation of a discarding policy. This policy serves the dual purpose of reducing congestion and selectively discarding corrupted or less critical packets, while ensuring a general level quality of the transmitted information.The congestion levels may also be influenced by the acknowledgment policy implemented by the recipient. In order to enhance efficiency, it is recommended that the receiver sends acknowledgment for many packets (N) instead of sending acknowledgement for each individual packet. The recipient is expected to transmit an acknowledgment only in the event that it has to send a packet using the piggybacking technique or when a timer reaches its expiration.The denial of new connections may occur when their establishment will result in network congestion. This process is sometimes referred to as admission control.

Closed Loop Congestion Control:

Closed loop congestion management strategies are used for the purpose of mitigating or resolving congestion after to its occurrence. Multiple approaches are used.

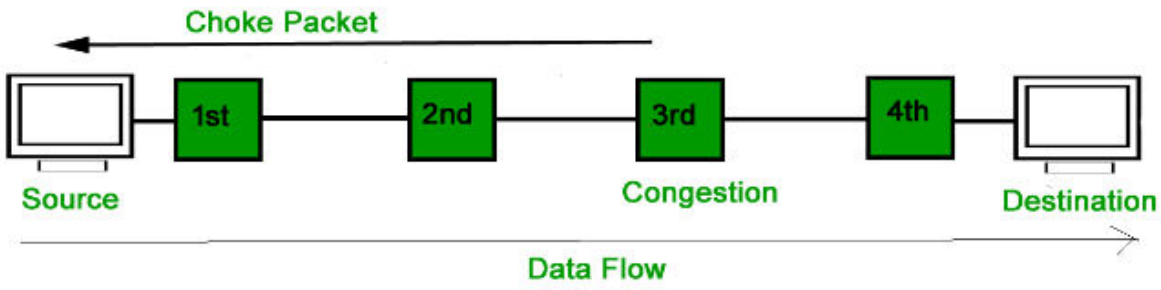
1.The concept of backpressure involves the implementation of a mechanism whereby a node that is experiencing congestion ceases to accept incoming packets from its upstream node. This phenomenon has the potential to result in congestion of the upstream node or nodes, leading to the refusal of data transmission from nodes situated higher in the network hierarchy. Backpressure is a congestion control strategy that operates at the node-to-node level and is characterised by the propagation of signals in the direction opposite to that of data flow.



In the figure shown, it can be seen that the third node has congestion, leading to a stop in the reception of packets. Consequently, the second node may also experience congestion as a consequence of the slowdown in the output data flow. Likewise, the first node may experience congestion and then notify the source to reduce its transmission rate.

2. A packet that a node sends to the source to alert it about congestion is known as a choke packet. Every router keeps an eye on the amount of resources it has and how each output line is being used.

When the administrator sets an acceptable level for resource utilisation, the router immediately sends a choke packet to the source as a way of asking it to cut down on traffic. There is no congestion alert sent to the intermediary nodes that the packets passed through.



3. There is no communication between the congested nodes and the source in implicit signalling. The source believes that a network is congested. For instance, one might assume that there is congestion if the sender transmits many packets and there is a delay in acknowledgment.

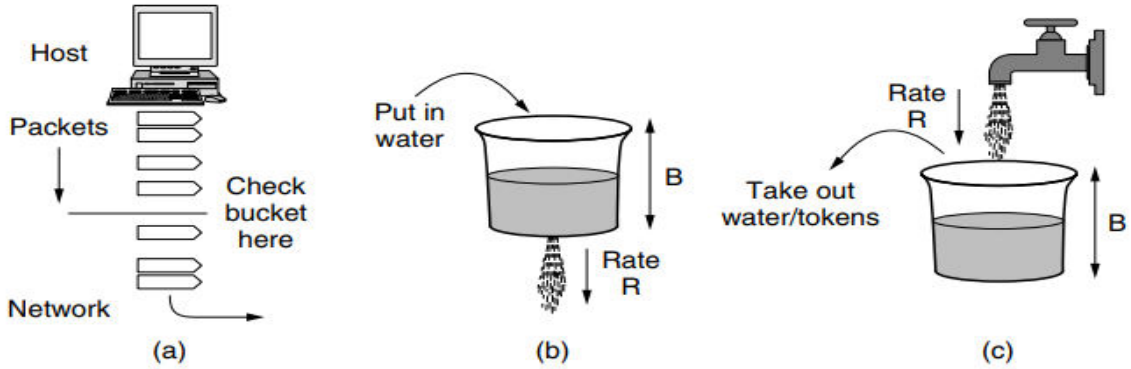
4. A router may tag each packet it transmits with a bit in the header to indicate congestion instead of creating more packets. When the network transmits the packet, the destination might observe congestion and notify the sender when it replies. As previously, the sender may restrict transmissions. This concept is used over the Internet and is known as ECN (Explicit Congestion Notification).If a packet has encountered congestion; it is indicated by two bits in the IP packet header.

5. If none of the aforementioned techniques relieve the congestion, routers have the ability to use load shedding. Load shedding is the technical term for routers discarding excessive amounts of packets they are unable to process. Which packets to discard is the crucial decision for a router that is overflowing with packets. Depending on the kind of applications using the network, a certain option could be used. An old packet has greater value than a fresh one during a file transfer. This is due to the fact that, for example, maintaining packets 7 through 10 and discarding packet 6 would merely make the receiver work harder to buffer data that it is not yet able to utilise. On the other hand, a fresh packet is worth more than an old one when it comes to real-time media. This is due to the fact that delayed packets lose their usefulness if they are not played by the required time.

6. Data networks see bursts of traffic. When the traffic rate fluctuates, it usually comes at nonuniform rates. A method for controlling the average speed and burstiness of a data flow entering the network is called traffic shaping. We shall now examine the token bucket and leaky bucket algorithms.

Leaky bucket Algorithm:

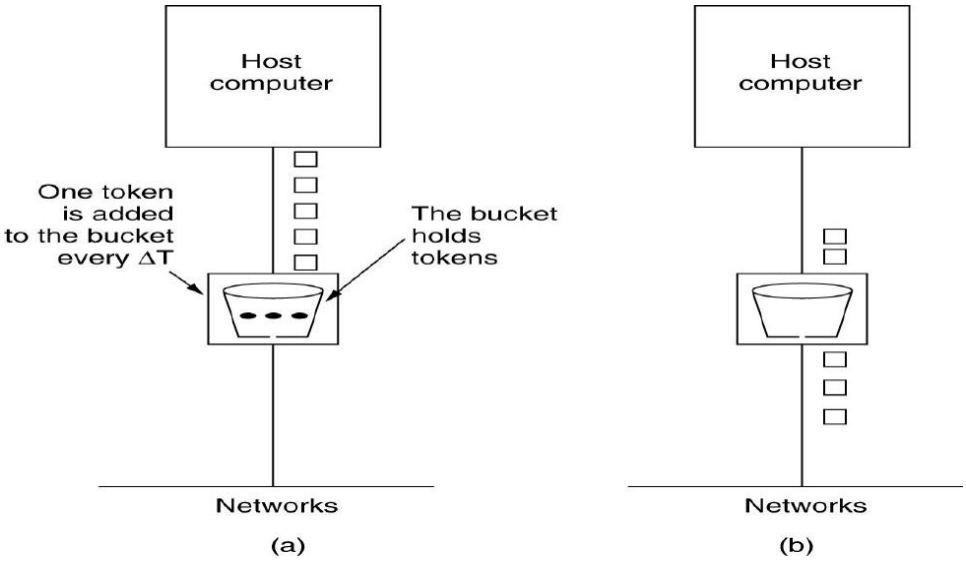
Consider a bucket with a little opening at the bottom. When there is any water in the bucket, the outflow is at a constant rate, R, regardless of the rate at which water enters the bucket; when the bucket is empty, the outflow is zero. Furthermore, any further water that enters the bucket after it reaches capacity B flows over the sides and is wasted.



Packets entering the network may be shaped using this bucket. Every host has an interface with a leaky bucket that connects it to the network. It must be feasible to add additional water to the bucket in order for a packet to be sent over the network. When a packet comes in after the bucket is full, it has to be threw or held off until enough water drains out to contain it.

Leaky bucket Algorithm: The Token Bucket Algorithm differs from the LB in that it permits the output rate to fluctuate based on the magnitude of the burst. In the TB algorithm, tokens are stored inside the bucket. In order to facilitate the transmission of a packet, the host is required to acquire and subsequently consume a single token. Tokens are produced by a timekeeping device at a frequency of one token per unit time, denoted as Δt seconds. Idle hosts have the capability to acquire and store tokens, accumulating them until the bucket reaches its maximum capacity. This accumulation allows hosts to subsequently transmit greater

bursts of data.



Internet Protocol

The main component that ensures the seamless functioning of the Internet is the network layer protocol known as IP (Internet Protocol).The transport layer is responsible for segmenting data streams into smaller units known as IP packets, which may then be sent.IP routers are responsible for the transmission of individual packets over the Internet, sequentially passing them from one router to the subsequent router, until the intended destination is successfully reached. Upon reaching the designated location, the network layer transfers the data to the transport layer, which then delivers it to the receiving process.Upon arrival at the target computer, the network layer undertakes the task of reassembling the constituent bits of the datagram, therefore restoring it to its original form. Subsequently, the datagram is transferred to the transport layer.A suitable point of departure for our examination of the network layer inside the Internet is the structure and composition of IP datagrams.The structure of an IPv4 datagram has two main components: a header section and a payload section.

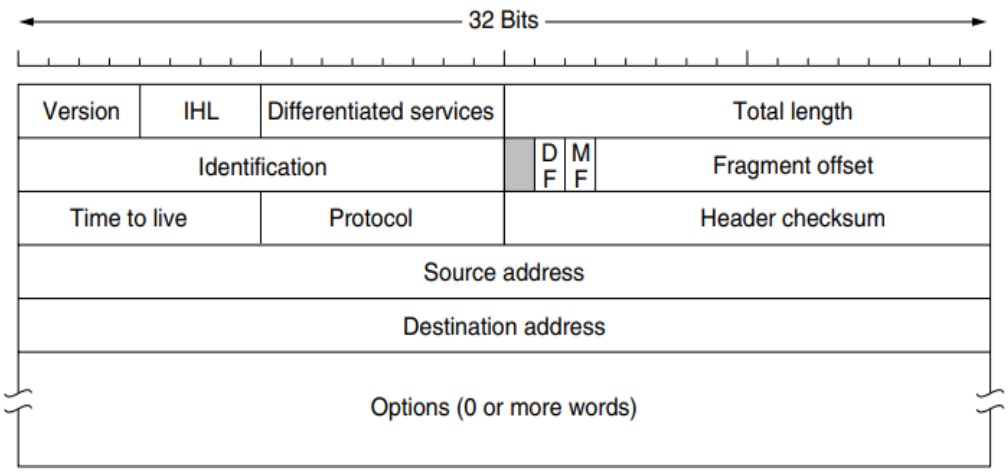


Figure 5-46. The IPv4 (Internet Protocol) header.

The 4 bit Version field is responsible for maintaining the details of the specific version of the protocol to which the datagram is associated. Currently, Version 4 is the main standard in the realm of the Internet.

IPv6, also known as Internet Protocol version 6, is the subsequent version of the IP protocol.

The format of an IPv4 address is represented as x.x.x.x, where each x is referred to as an octet and is required to be a decimal number ranging from 0 to 255. In computer networking, octets are often separated by periods. An IPv4 address is required to consist of four octets separated by three periods.

Example: 01.102.103.104

The standard format for an IPv6 address consists of eight segments, denoted as y:y:y:y:y:y:y:y. Each segment, referred to as "y," represents a hexadecimal number ranging from 0 to FFFF.

The IHL is a 4-bit field is used to indicate the length of the header.

The minimum value of 5 is applicable in cases when none of the options are provided.

The maximum possible value of the 4-bit field is 15, hence imposing a constraint on the header size, which is restricted to 60 bytes.

The minimal length of the header is 20 bytes.

The maximum value for the length of the header is 60 bytes.

The maximum payload value, including the header length, is 65535 bytes.

An increase in the length of the header results in a corresponding reduction in the size of the payload.

The Differentiated Services (DS), which utilises 8 bits, is responsible for specifying the Type of Service. Different combinations of reliability and speed may be achieved.

In the context of digitised voice, quick delivery surpasses precise delivery. In the context of file transfer, ensuring error-free transmission takes prominence over speedy transmission.

The Type of Service field allocates 3 bits for indicating priority and a further 3 bits for indicating the host's preference towards latency, throughput, or reliability.

There are still two remaining bits that constitute Explicit Congestion Notification (ECN).

The total length of the datagram, which consists of both the header and data, is 16 bits. The upper limit of the length is 65,535 bytes.

The inclusion of the Identification field is necessary in order to enable the recipient determine the specific packet to which a recently received fragment corresponds. All fragments inside a packet possess identical Identification values.

Subsequently, an unutilized bit follows, creating a sense of surprise. This particular bit is used for the purpose of identifying and discerning potentially harmful network traffic. The proposed approach would significantly enhance security measures by enabling the identification and subsequent rejection of packets containing the designated 'evil' bit, hence establishing their origin as malicious entities.

Next, there are two 1-bit feilds that relate to fragmentation. The acronym DF is an abbreviation for the term "Don't Fragment." The directive instructs the routers to keep away from fragmenting the packet.

Initially, the purpose was to provide assistance to hosts who lacked the ability to reassemble the fragments. The acronym MF denotes More Fragments.

The fragment offset indicates the specific position inside the current packet to which this fragment corresponds.

The Time to Live (TTL) field, consisting of 8 bits, serves as a counter that is used to restrict the lifespan of packets.

The initial intention was for the time measurement to be in seconds, with a maximum duration of 255 seconds. The value must be reduced by one with each iteration. Once the packet's value reaches zero, it is deleted and a warning message is then sent back to the originating host. This functionality serves to prevent packets from indefinitely traversing the network.

Once the network layer has successfully aggregated all the necessary components of a packet, it is essential for it to choose the appropriate course of action for the packet. The Protocol field is responsible for determining the appropriate transport mechanism to which the packet should be directed. One potential option is Transmission Control Protocol (TCP), however, User Datagram Protocol (UDP) and other alternatives also exist. The Header checksum is assigned to the header in order to safeguard critical information, such as addresses, by providing a means of verification.

The Source address and Destination address serve to denote the Internet Protocol (IP) address of both the source and destination, respectively.

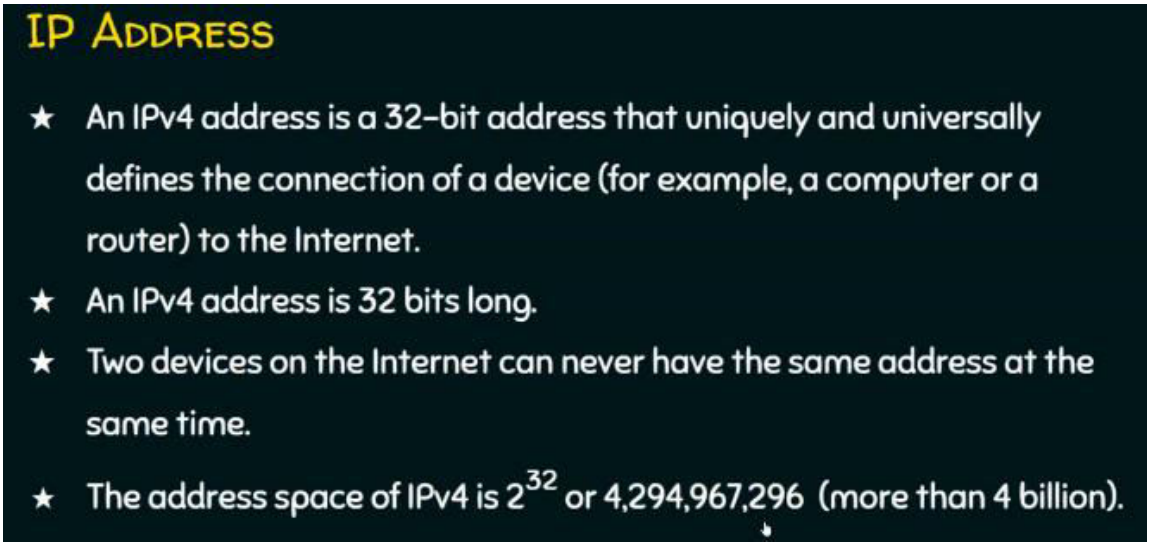
IP Addresses

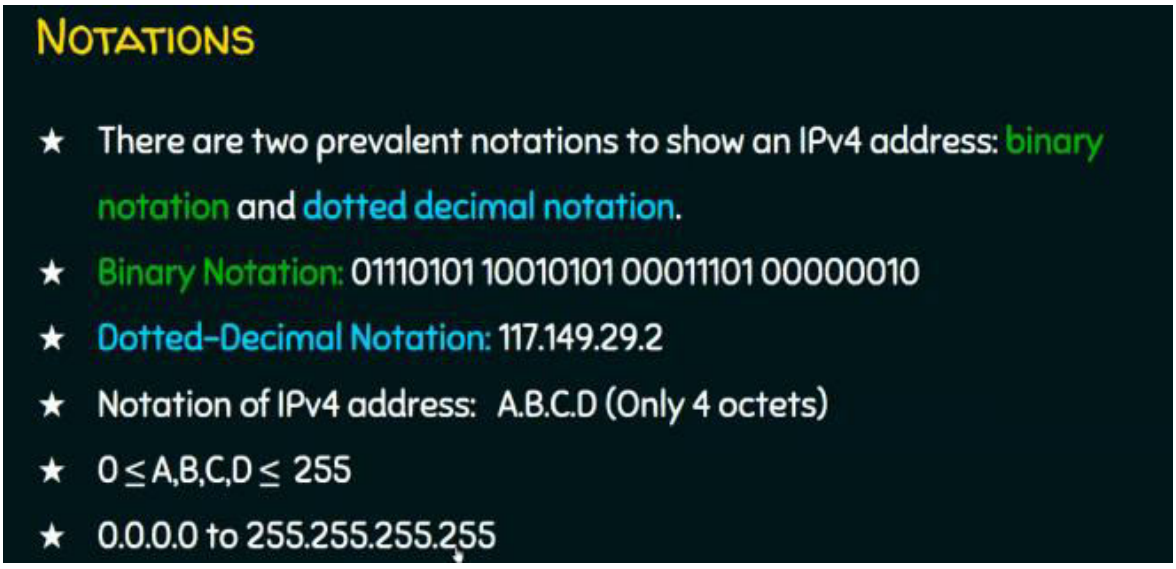
IPv4 is identified by its 32-bit addresses. The Source address and Destination address sections of IP packets may be filled with the IP address of any host or router connected to the Internet.

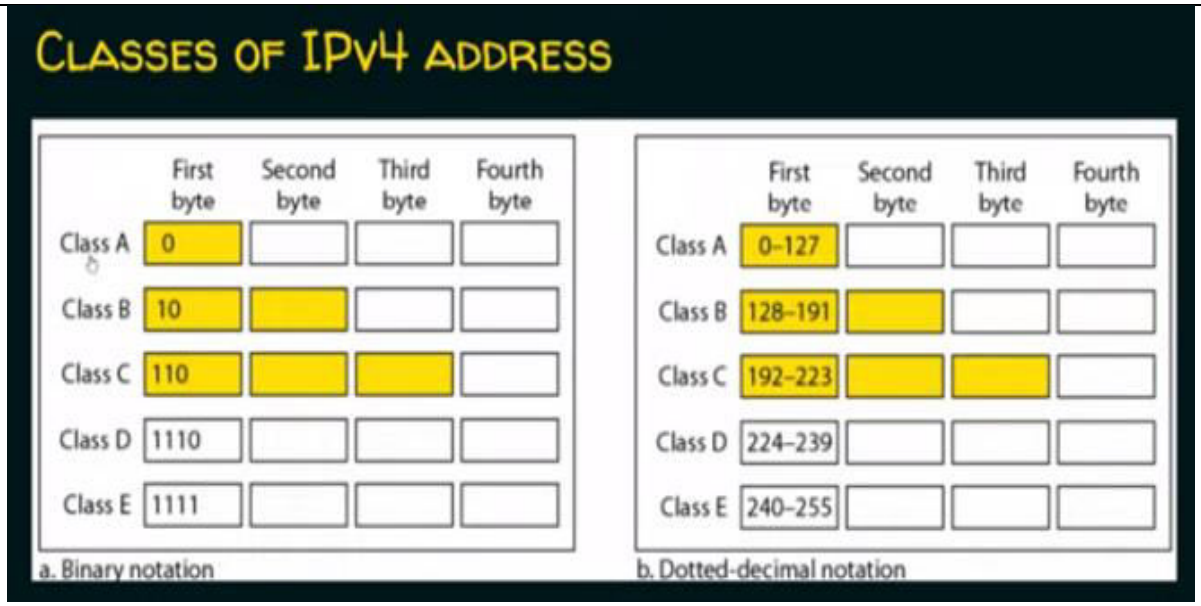
It's crucial to remember that an IP address does not really correspond to a host. In actuality, it refers to a

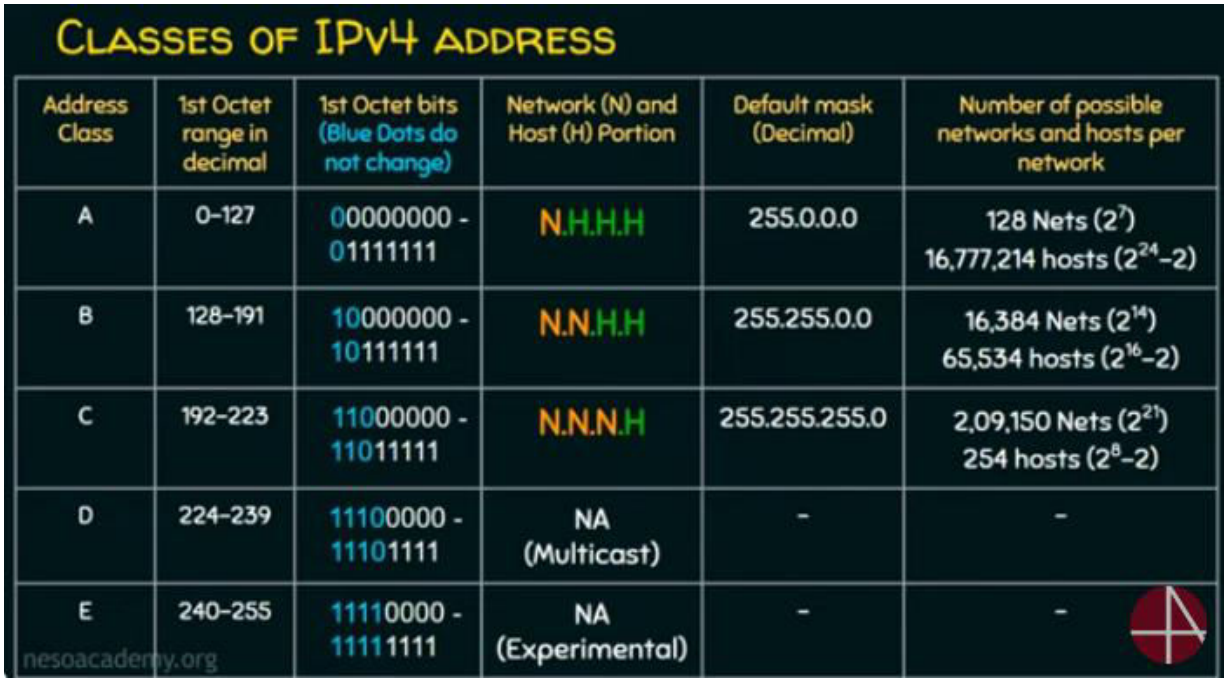
network interface.A host component resides in the bottom bits of every 32-bit address, while a variable-length network portion occupies the top bits.For every host on a single network, the network portion has the same value.

This indicates that an IP address space block that is contiguous to a network belongs to it. We refer to this block as a prefix.The format used to write IP addresses is dotted decimal.Each of the four bytes in this format is represented in decimal, ranging from 0 to 255.









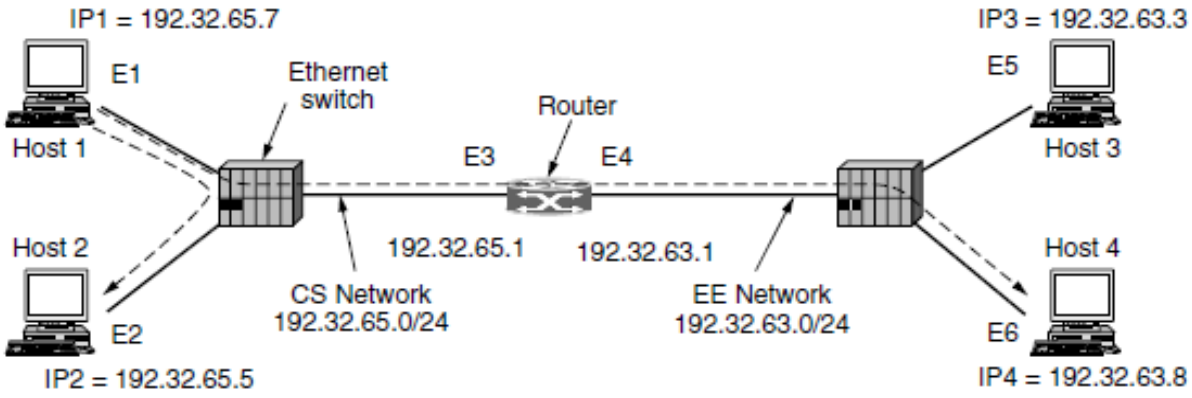
Internet control protocols

The **Internet Control Message Protocol (ICMP)** is a network protocol that is used to provide error messages and functional information about network conditions.In addition to the Internet Protocol (IP), which serves as the primary means for data movement, the Internet has a variety of complementary control protocols that operate at the network layer.The protocols included in this category are ICMP, ARP, and DHCP.

The routers carefully monitor the functioning of the Internet.In the case of an unforeseen occurrence during the processing of packets at a router, the ICMP (Internet Control Message Protocol) is responsible for notifying the sender.

ARP—The Address Resolution Protocol:

Even though every computer connected to the Internet has one or more IP addresses, transmitting packets requires more than just these addresses. Internet addresses are not understood by data link layer NICs (Network Interface Cards), such as Ethernet cards. When it comes to Ethernet, each and every NIC that has ever been produced has a unique 48-bit Ethernet address. To make sure that no two Ethernet network interface controllers have the same address, Ethernet NIC manufacturers ask IEEE for a block of Ethernet addresses.48-bit Ethernet addresses are used by the NICs to transmit and receive frames. They have no knowledge whatsoever about 32-bit IP addresses.



Now, host 1's upper layer software creates a packet and sends it to the IP software for transmission, adding 192.32.65.5 to the destination address field. The destination is on the CS network, which is its own network, as the IP programme can determine by looking at the address. To transmit the frame, it still requires a method to determine the destination's Ethernet address. Having a configuration file that maps IP addresses to Ethernet addresses someplace in the system is one way to solve this problem. While there is no doubt that this technique is feasible, maintaining all these files up to date is a laborious and error-prone task for organisations with thousands of devices.

A better way would be for host 1 to query who owns IP address 192.32.65.5 via a broadcast packet sent over the Ethernet. Every computer connected to the CS Ethernet will receive the broadcast and verify its IP address. Only Host 2 will reply, providing its Ethernet address (E2). In this manner, host 1 discovers that the host with Ethernet address E2 has IP address 192.32.65.5. ARP is the name of the protocol that is used to pose this query and get a response (Address Resolution Protocol).

The Dynamic Host Configuration Protocol:

Hosts are equipped with fundamental details, such as their own IP addresses. By what means do hosts get this information? Manual configuration of individual computers is a feasible approach; nonetheless, this method is characterised by its time-consuming nature and susceptibility to errors. An alternative method, known as Dynamic Host Configuration Protocol (DHCP), exists. In the context of networking, it is important

for each network to possess a Dynamic Host setup Protocol (DHCP) server, which assumes the responsibility of network setup. The computer initiates a transmission to request an IP address inside its network. This is achieved by the use of a DHCP DISCOVER packet. It is essential that this packet reaches the Dynamic Host Configuration Protocol (DHCP) server. Upon receiving the request, the server proceeds to assign an available IP address and transmits it to the host via a DHCP OFFER packet. In order to do this task in situations when hosts lack IP addresses, the server employs the identification of a host by its Ethernet address, which is sent inside the DHCP DISCOVER packet. One concern that arises in the context of automated allocation of IP addresses from a pool is the duration for which an IP address should be assigned. In the event that a host departs from the network without surrendering its IP address to the DHCP server, the said address will be irretrievably forfeited. Over the course of time, it is possible for a considerable number of addresses to get lost or misplaced. In order to mitigate this occurrence, the allocation of IP addresses might be implemented for a predetermined duration, using a method known as leasing. Immediately before to the termination of the lease, it is essential for the host to initiate a request for DHCP renewal. In the event of a failed request or a refused request, the host is no longer permitted to utilise the previously assigned IP address.