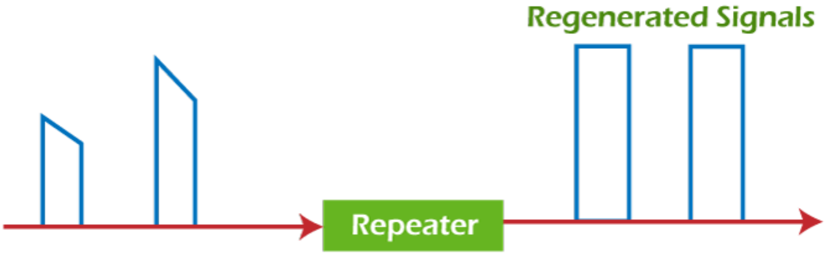
Unit 4

B230503T Data and Communication Networks

Devices:
Repeaters, bridges, gateways, routers, The Network Layer; Design Issues, Routing algorithms, Congestion control Algorithms, Quality of service, Internetworking, Network-Layer in the internet. Transport and upper layers in OSI Model' Transport layer functions, connection management, functions of session layers, presentation layer and application layer.

Repeater:



The *repeater repeats the signal from the transmitter and supplies it to another repeater with high power gain*. The amplifier circuit is another component of the repeater. Additionally, a repeater can be created to fit the characteristics of the communication system. We require repeater with a photo detector and other light-sensitive hardware for optical communication. On the other hand, while working with electromagnetic signals, signal regeneration requires using antennas, waveguides, etc.

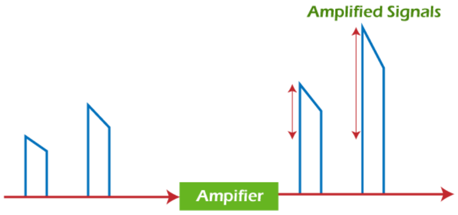
Due to its superior ability to handle digital signals, a repeater is an essential component of the digital communication system. We might be wondering what exactly qualifies a repeater as a crucial tool that can be trusted to be used in digital communication systems.

An electronic device known as a repeater only operates on the physical layer of the OSI model. Signals travelling from one host to another carry the data during transmission over the network. The information-carrying signals can only travel a certain distance via the network due to signal attenuation that can cause the loss of all or part of the information as the signal travels.

Attenuation is generated because the medium through which the signal is travelling produces some kind of resistance. Hence, to solve the attenuation problem, a repeater is installed on a link that receives the signal before it reaches its limits or becomes incredibly weak. When a signal comes in, the repeater listens for it, regenerates the original bit pattern-not the noise- and retransmits the signal into the system.

A repeater only offers a way to *increase the network's actual length*. It does not alter any of the network's operations and lacks the intelligence to stop or reroute an incoming frame on a different path.

Amplifier:

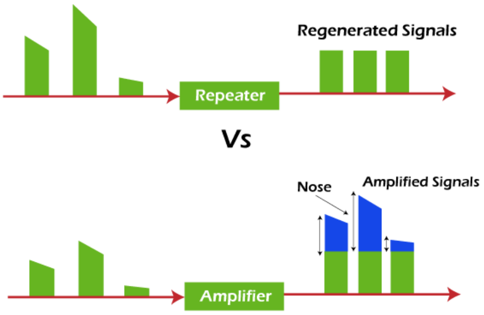


An amplifier is an electronic device, whose goal is to increase the amplitude of the signal waveform without changing its frequency or wave shape. It is one of the electronic circuits used the most frequently and can serve a variety of purposes. Typically, wireless communication uses amplifiers.

When a signal that has already been transmitted is found to be weak, an amplifier is used *to* raise the signal's amplitude *or* intensity. It produces high output power while requiring little input electricity.

The Amplifier contains transistors and capacitors that are used to link the signal from one circuit to another. The DC power source provides the amplifier with the energy it needs to magnify the distorted signal.

Difference between Repeater and Amplifier:



Parameter	Repeater	Amplifier
Definition	The repeater is used to repeat the signal numerous times between the transmitter and receiver.	The amplifier is used to increase the amplitude of the weak signal.
Usage	In order to repeat digital signals, repeaters are utilised.	Amplifiers are mostly utilised in communication systems which contains analog signal.
Installation Distance	Repeaters are typically required because, digital signals fade quickly in contrast to analog signals. Therefore, the number of repeaters needed in the communication system will be more than the number of amplifiers.	There can be a sufficient distance between two amplifiers due to the slow decay of analog signals.
Noise Elimination	Because repeaters alter the signal, they are effective at reducing noise.	The resultant signal is noisier because the amplifier amplifies

		both the information and noise signals simultaneously.
Outcome of using the device	Maximises the signal-to-noise ratio, which reduces the signal's related error.	Reduces the signal-to- noise ratio, which raises the noise.
Properties	High gain and low output power.	Low gain and high output power.

Key Differences between Repeater and Amplifier:

❖The repeater is used to regenerate the original signal using the received signal pattern and retransmitting the regenerated signal. The amplifier, on the other hand, amplifies the signal by raising its amplitude.

❖The repeater has a high gain power and low output power. On the other hand, Amplifiers have low gain power and high output power.

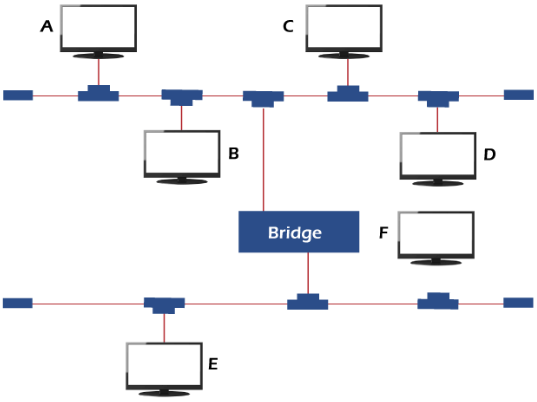
❖The amplifier increases the signal power with embedded noise since it is unable to distinguish between the intended signal and noise. The repeater, in contrast, eliminates signal noise while, bit by bit, regenerating the signal.

❖The amplifiers' implications lead to a reduced signal-to-noise ratio and more noise. In contrast, repeaters raise the signal-to-noise ratio, lowering the signal's associated error.

❖In a stationary environment where the radio frequency signal is steady, like buildings, repeaters are utilised. Contrarily, amplifiers are utilised in a mobile environment such as remote areas, where the radio signal is weak and constantly varying.

Bridge:

A bridge is a networking device that works in both the physical and data link layer in a network. These devices can divide a large network into smaller segments and pass the frames between two originally separated LANs. A bridge maintains a MAC address of various stations attached to it. When a frame enters a bridge, it checks the address contained in the frame and compares it with a table of all the stations on both segments.

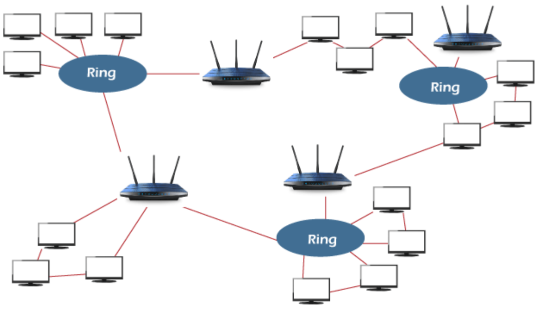


A Bridge

For Example, A-frame is sent from station A to station C. When this frame arrives at the Bridge, the Bridge checks its table and blocks it from crossing into the lower segment as station C is in the upper segment only. Thus, a frame is relayed to the entire upper segment and is not allowed to move to lower segment. If the frame is to be transmitted from station A to station F, the Bridge will allow this frame to pass through it and relay it to the entire lower segment.

Router:

It is an interconnecting device that works at the physical, data link and network layer of OSI reference model. It may connect LAN and WAN in the network and can pass or relay the packets among them. It has access to the network or logical address. The following figure displays the router acts as a station in the network.



Routers is an internet

In this the routers are a member of more than one network simultaneously. They have links with two or more networks and contain the addresses of the stations on all these networks. It receives the packets from one connected network and passes them to a second connected network. If a received packet contains the address of a node that is on some other network, the Router determines which of its connected networks the best next relay point for that packet.

Following are the point-to-point comparison between Router and Bridge:

Sr. No	Points of differences	Router	Bridge
1	**Function**	The main function is to route the packets and to reduce the network problems.	The main function of Bridge is to filter the packets and to keep the traffic for each segment separately.
2	**Layers**	It is a hardware device that works at the network, data link & physical layer of the OSI Model.	It is a hardware device that works at the OSI model's data link and physical layer.
3	**Address**	The Router has access to the logical address or IP address of stations.	The Bridge has access to a physical address or MAC address of stations.

4	**Protocols**	RIP, OSPF, etc. these are some protocols that can be configured in the Router.	In Bridge, there are no protocols to configure.
5	**Connection**	It connects two or more networks and routes packets between them.	The Bridge is used to extend the existing network or divide or large network into smaller segments.
6	**Routing Table**	The Router uses a routing table to store information. This table is dynamic and is updated using routing protocols.	The Bridge does not use a routing table for storing information.
7	**Data Structure**	A router used graph data structure.	Bridge used tables data structures
8	**Network Segmentation**	In Router enables network segmentation.	In Bridge network segmentation is disable.
9	**Domain**	It works on more than single broadcast domains.	Bridge works on a single broadcast domain.
10	**Transparency**	It is not transparent to the end stations.	It is transparent to the end stations and do not rely on the protocol.
11	**Efficiency**	Routing is more efficient.	The Bridge has less efficiency than the Router.
12	**Ports**	It has more than two ports.	It has only two ports.
13	**Path**	Router devices can accommodate multiple paths.	Bridge devices can accommodate a single path.
14	**Setup**	Difficult	Easy
15	**Cost**	Routers are relatively expensive devices.	Bridges are relatively inexpensive devices.

What is Gateway?

A gateway is simply a device or hardware that acts as a **"gate"** between the networks. We can also define it as a node that acts as an entry for other network nodes. It is also responsible for facilitating the traffic flow within the network. Gateway uses more than one communication protocol, so its activities are more complicated than a router or a switch.

Gateways is essentially a system used to communicate between networks with different protocols and are responsible for converting one protocol into another. The gateway is a computer device that's responsible for routing traffic from the primary workstation to the outside network for every workplace form. It is responsible for providing access to the internet for households, thereby serving as an internet service provider.

Main Differences between the Router and Gateway:

Here, we are going to discuss the main differences between the Router and Gateway.

The complexity of the Components:

The single access point in the gateway outside the network is the main difference between router and gateway. Based on the gateway's criticality, it either serves as a server with the gateway application installed or acts as a linking mechanism to others between several computer networks. The two networks should have a gateway that allows the networks to communicate as an entry and exit endpoint if any N network wants to reach the M network. Gateways are doors to the network that determine the network's boundaries and edges. In comparison, routers determine the minimum possible distance from computer M to computer N to be transported by data packets.

Security:

Routers have to be secluded from being filled with massive data and heavy traffic. It is important to ensure that congestion between the routing paths can be minimized acceptably, so several routing tables should be designed to map the network's data travel process. Whereas the gateway is important, since it is the endpoint for the network, it should be highly protected to avoid a virus attack. The data passes via the gateway could be easily accessed. If a single router is flooded or granted, the particular router can be disabled by the customer. In order to get the data over the network, another router determines the shortest possible way. However, if the user eliminates the gateway, it leads to the whole down of the network.

Components Configuration:

The routers are designed with a list of IP addresses from the routing tables that can transfer the router data. While the gateway is configured by specifying the recommended internal and external IP addresses, it has two ports to iterate between routers and gateways for internal and external IPs.

Routing and Managing the Traffic Flow:

The two devices are used to monitor network traffic between two or more different networks. However, a minimum of two network cards can be applied in the system if the user finds it difficult to manage traffic. The gateway handles traffic between two similar networks easily, while routers control the same network's traffic flow.

Head to Head Comparison between the Router and Gateway:

Let us discuss the head to head comparison between Router and Gateway through the below tabular form.

Features	Router	Gateway
Definition	A Router is a networking layer system used to manage and forward data packets to computer networks.	A gateway is simply a device or hardware that acts as a "**gate**" between the networks. It could also be defined as a node that acts as an entry for other network nodes.
Working	Usually, routers run on the 3rd	Gateway interprets the network system as

Principle	layer of the protocol and transmit the packets from one system to another. A router chooses the network's path to transport the data packets.	endpoints from one packet to another.
Hosting	It is available only to dedicated applications.	It is hosted on the dedicated application, physical servers, and virtual applications.
Networks	It routes the data packets via similar networks.	It connects two dissimilar networks.
Deployment	It is deployed on the router hardware in a specific appliance.	The gateway is deployed as the virtual or physical server or the specific appliance.
OSI Layer	It can operate only on **3** and **4** layers.	It can operate only on the **5** layers.
Dynamic Routing	Router supports dynamic routing.	Gateway doesn't support dynamic routing.
Associated terms	The router is also called a wireless router and an Internet router.	The gateway is also called a gateway router, proxy server, and voice gateway.
Component's Operating Process	The router operates by installing different routing data for different networks, and the destination address is based on traffic.	The gateway works by distinguishing between the network structure and the components available outside the network.

Network Layer:

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

The main functions performed by the network layer are:

Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.

Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

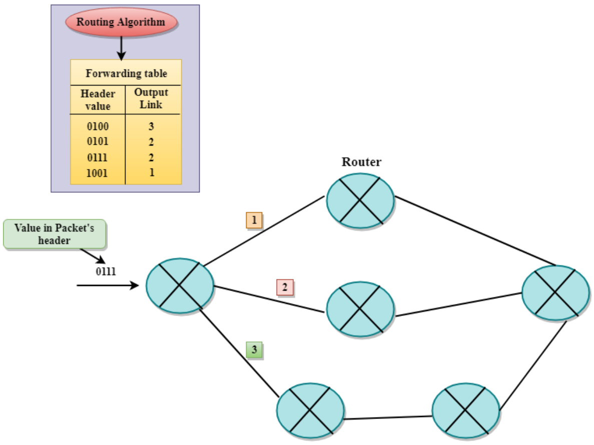
Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.

Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Forwarding & Routing:

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

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



Routing algorithms determine the values in forwarding table

Services Provided by the Network Layer:

Guaranteed delivery: This layer provides the service which guarantees that the packet will arrive at its destination.

Guaranteed delivery with bounded delay: This service guarantees that the packet will be delivered within a specified host-to-host delay bound.

In-Order packets: This service ensures that the packet arrives at the destination in the order in which they are sent.

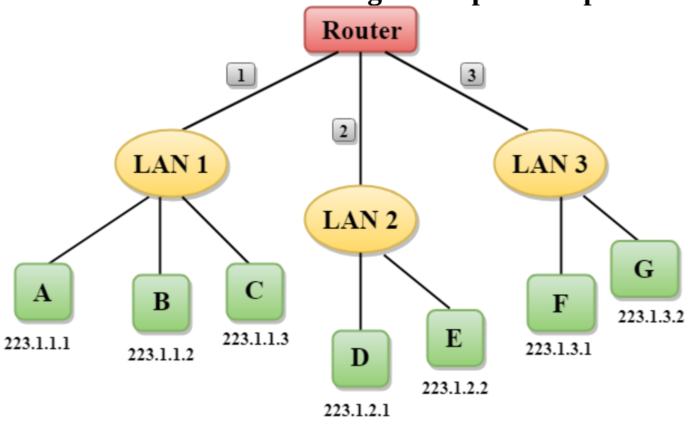
Guaranteed max jitter: This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.

Security services: The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Network Addressing:

❖Network Addressing is one of the major responsibilities of the network layer.
❖Network addresses are always logical, i.e., software-based addresses.
❖A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
❖A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
❖Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Let's understand through a simple example.



In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.

Each host contains its own interface and IP address.

All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.

Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing:

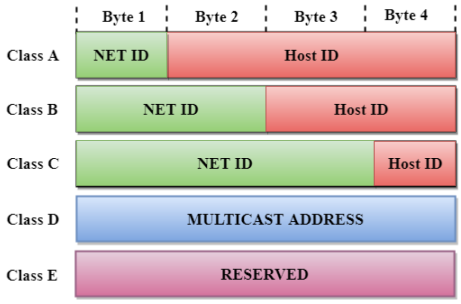
An IP address is 32-bit long. An IP address is divided into sub-classes:

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

An IP address is divided into two parts:

Network ID: It represents the number of networks.

Host ID: It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

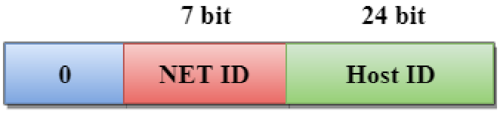
In Class A, an IP address is assigned to those networks that contain a large number of hosts.

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

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address



Class B

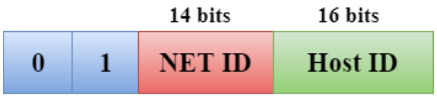
In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address



Class C

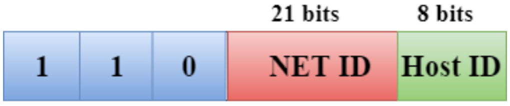
In Class C, an IP address is assigned to only small-sized networks.

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

In Class C, the higher order bits of the first octet are always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

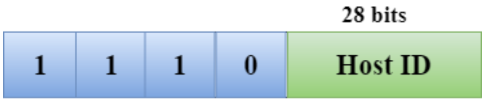
The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^8 - 2 = 254 host address



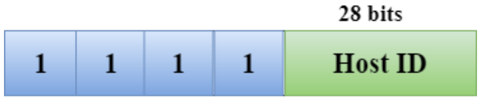
Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet are always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Classful Network Architecture:

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 223.255.255.25

						5
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

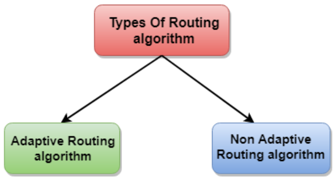
Routing algorithm:

- 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.
- 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.
- 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.
- 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:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm


Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

Adaptive Routing algorithm:

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- 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:

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. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

Isolation algorithm: It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.

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:

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- 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:

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.

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.

What is Congestion Control Algorithm?

Congestion causes choking of the communication medium. When too many packets are displayed in a method of the subnet, the subnet's performance degrades. Hence, a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

There is two congestion control algorithm which is as follows:

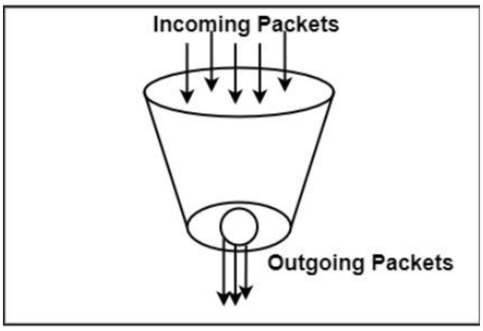
Leaky Bucket

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting. The algorithm allows controlling the rate at which a record is injected into a network and managing burstiness in the data rate.

A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms. This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.

The figure shows the leaky bucket algorithm.

Leaky Bucket Algorithm



In this algorithm, a bucket with a volume of, say, b bytes and a hole in the Notes bottom is considered. If the bucket is null, it means b bytes are available as storage. A packet with a size smaller than b bytes arrives at the bucket and will forward it. If the packet's size increases by more than b bytes, it will either be discarded or queued. It is also considered that the bucket leaks through the hole in its bottom at a constant rate of r bytes per second.

The outflow is considered constant when there is any packet in the bucket and zero when it is empty. This defines that if data flows into the bucket faster than data flows out through the hole, the bucket overflows.

The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources. The leak rate is a fixed parameter. In the case of the traffic, volume is deficient, the large area of network resources such as bandwidth is not being used effectively. The leaky-bucket algorithm does not allow individual flows to burst up to port speed to effectively consume network resources when there would not be resource contention in the network.

Token Bucket Algorithm

The leaky bucket algorithm has a rigid output design at the average rate independent of the bursty traffic. In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.

It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket. The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.

When tokens are shown, a flow to transmit traffic appears in the display of tokens. No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Thus, the token bucket algorithm adds a token to the bucket each 1 / r seconds. The volume of the bucket is b tokens. When a token appears, and the bucket is complete, the token is discarded. If a packet of n bytes appears and n tokens are deleted from the bucket, the packet is forwarded to the network.

When a packet of n bytes appears but fewer than n tokens are available. No tokens are removed from the bucket in such a case, and the packet is considered non-conformant. The non-conformant packets can either be dropped or queued for subsequent transmission when sufficient tokens have accumulated in the bucket.

They can also be transmitted but marked as being non-conformant. The possibility is that they may be dropped subsequently if the network is overloaded.

What is Quality of Service (QOS)?

Quality of Service (QOS) determines a network's capability to support predictable service over various technologies, containing frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET IP-routed networks. The networks can use any or all of these frameworks.

The QOS also provides that while supporting priority for one or more flows does not create other flows fail. A flow can be a combination of source and destination addresses, source and destination socket numbers, session identifier, or packet from a specific application or an incoming interface.

The QOS is primarily used to control resources like bandwidth, equipment, wide-area facilities etc. It can get more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc.

QOS Concepts:

The QOS concepts are explained below:

Congestion Management

The bursty feature of data traffic sometimes bounds to increase traffic more than a connection speed. QoS allows a router to put packets into different queues. Servicespecific queues more often depend on priority than buffer traffic in an individual queue and let the first packet by the first packet out.

Queue Management

The queues in a buffer can fill and overflow. A packet would be dropped if a queue is complete, and the router cannot prevent it from being dropped if it is a high priority packet. This is referred to as tail drop.

Link Efficiency

The low-speed links are bottlenecks for lower packets. The serialization delay caused by the high packets forces the lower packets to wait longer. The serialization delay is the time created to put a packet on the connection.

Elimination of overhead bits

It can also increase efficiency by removing too many overhead bits.

Traffic shaping and policing

Shaping can prevent the overflow problem in buffers by limiting the full bandwidth potential of the applications packets. Sometimes, many network topologies with a highbandwidth link connected with a low-bandwidth link in remote sites can overflow low bandwidth connections.

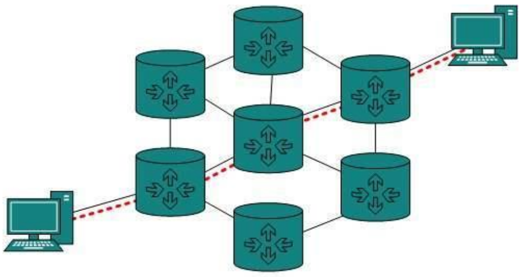
Therefore, shaping is used to provide the traffic flow from the high bandwidth link closer to the low bandwidth link to avoid the low bandwidth link's overflow. Policing can discard the traffic that exceeds the configured rate, but it is buffered in the case of shaping.

Internetworking in Computer Network:

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

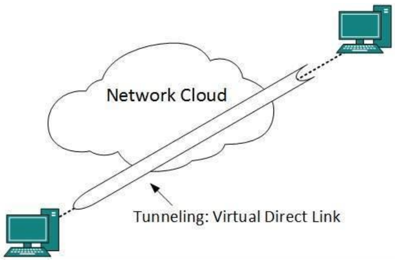


Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Tunneling

If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

Packet Fragmentation

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

If a packet with DF (don't fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

The Internet Layer in the TCP/IP Model

The Internet layer is responsible for logical transmission of data packets over the internet. It can be compared to the network layer of the OSI model.

The main functions of the internet layer are:

- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- It reassembles the out-of-order packets when they reach the destination.
- It handles the error in transmission of data packets and fragmentation of data packets.

The protocols used in this layer are:

Internet Protocol, IP − It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called datagrams that travel over different routes across multiple nodes.

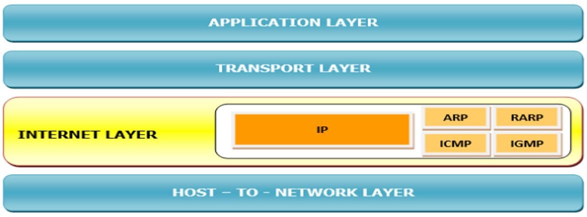
Address Resolution Protocol, ARP −This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.

Reverse Address Resolution Protocol, RARP − This is to find the Internet address of a host when its physical address is known.

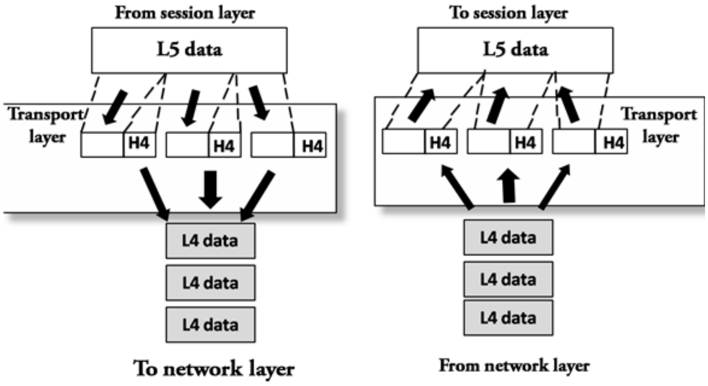
Internet Control Message Protocol, ICMP − It monitors sending the queries as well as the error messages.

Internet Group Message Protocol, IGMP −It allows the transmission of a message to a group of recipients simultaneously.

The following diagram shows the network layer in the TCP/IP protocol suite:



Transport Layer:



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

Transmission Control Protocol

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

User Datagram Protocol

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

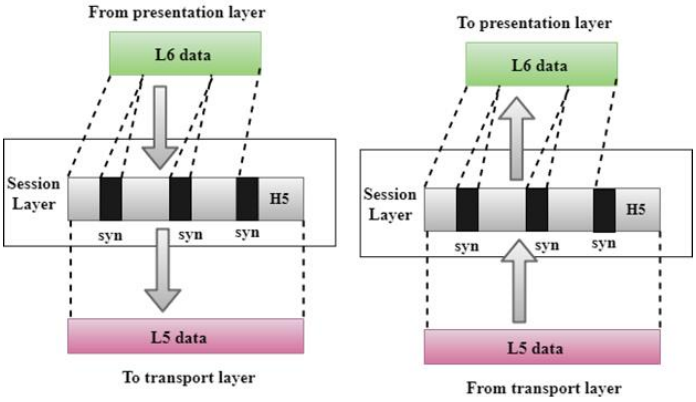
Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

Flow control: The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer:



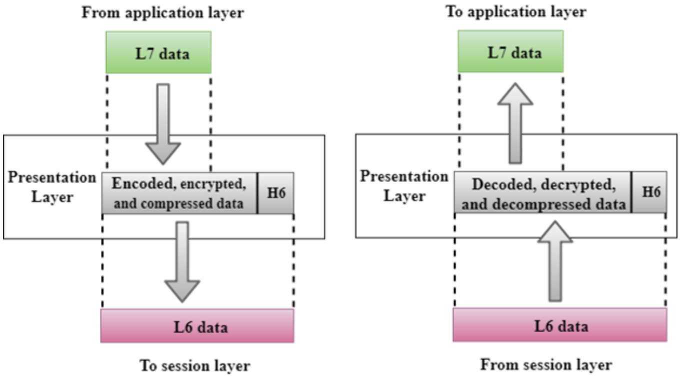
- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer:



- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

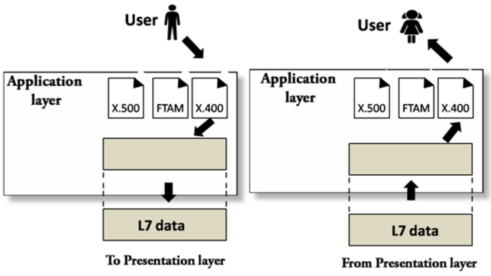
Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer:

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.



Functions of Application layer:

File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

Mail services: An application layer provides the facility for email forwarding and storage.

- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.