**Q.1 What is the difference between a token bucket and leaky bucket algorithm?**

**Ans:**

• Traffic shaping (also referred to as packet shaping) is the technique of delaying and restricting certain packets travelling through a network to increase the performance of packets that have been given priority.

• Classes are defined to separate the packets into groupings so that they can each be shaped separately allowing some classes to pass through a network more freely than others. Traffic shapers are usually placed at the boundaries of a network to either shape the traffic going entering or leaving a network.

• Traffic shaping is a mechanism to control the amount and rate of the traffic sent to the network. The two traffic shaping techniques are:

1. Leaky Bucket
2. Token Bucket

|  |  |
| --- | --- |
| **Token Bucket** | **Leaky Bucket** |
| Token dependent |  Token independent |
|  If the bucket is full token is discarded, but not the packet. |  If the bucket is full packet or data are discarded |
|  Packets can only send when there is enough token |  Packets are transmitted continuously |
|  It allows large bursts to be sent faster rate after that constant rate. |  It sends the packet at a constant rate. |
|  It saves token to send large bursts |  It does not save the token. |
|  Token Bucket does not have discard or priority policy |  Leaky Bucket has priority policy |
|  Burstiness is bounded as follows: - Flow never sends more than β+T∗ρ β+T∗ρ tokens worth of data in interval τ and - Long-term transmission rate will not exceed ρ | * The flow never sends faster than ρ worth of packets per second |

**Q.2 Differentiate between open loop and closed loop congestion control methods?**

**Ans:**

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**

Open-loop congestion control policies are applied to prevent congestion before it happens. The congestion control is managed either by the source or the destination. Types of Open Loop Congestion control:

1. **Retransmission Policy:**

It is the policy in which retransmission of the packets is taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and able to perfect efficiency.

1. **Window Policy**:

The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse. Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

1. **Discarding Policy:**

A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and able to keep the quality of a message. In case of audio file transmission, routers can discard fewer sensitive packets to prevent congestion and keep the quality of the audio file.

1. **Acknowledgement Policy:**

Since acknowledgement is also the part of the load in-network, the acknowledgement policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgement. The receiver should send an acknowledgement for N packets rather than sending an acknowledgement for a single packet. The receiver should send an acknowledgement only if it has to send a packet or a timer expires.

1. **Admission Policy:**

In admission policy, a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion or there is congestion in the network, the router should deny setting up a virtual network connection to prevent further congestion.

* **CLOSED-LOOP CONGESTION**

The closed-loop congestion control technique is used to treat or alleviate congestion after it happens. Types of Closed Loop Congestion control:

**Backpressure:** Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.  The backpressure technique can be applied only to virtual circuit networks. In such a virtual circuit, each node knows the upstream node from which data flow is coming. In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

**Choke Packet:**In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion. Here, the congested node does not inform its upstream node about the congestion as in backpressure method. In the choke packet method, the congested node sends a warning directly to the source station *i.e.*the intermediate nodes through which the packet has travelled are not warned.

**Implicit Signaling:** In implicit signalling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgement. Therefore, the delay in receiving an acknowledgement is interpreted as congestion in the network. On sensing this congestion, the source slows down. TCP uses this type of congestion control policy.

**Explicit Signaling:** In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion. Explicit signalling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose while, in explicit signalling method, the signal is included in the packets that carry data. Explicit signalling can occur in either the forward direction or the backward direction. In backward signalling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down. In forward signalling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver, in this case, uses policies such as slowing down the acknowledgements to remove the congestion.

|  |  |  |  |
| --- | --- | --- | --- |
| Sr.no | Point of Difference | Closed-loop control system | Open-loop control system |
| 1 | Definition | Change in output affects input | No change in input with a change in output |
| 2 | Feedback loop | Present | Not Present |
| 3 | Error Correction | Possible | Not possible |
| 4 | Accuracy | Fully accurate | Inaccurate |
| 5 | Bandwidth | Large | Small |
| 6 | Stability | Stability should be considered during designing | Stable |
| 7 | Construction | Complex | Simple |
| 8 | Sensitivity to noise | Less sensitive | Extremely sensitive |
| 9 | Effect of non-linearities | Effect is reduced | Highly affected |
| 10 | Block Diagram |  |  |
| 11 | Examples | Missile launching system, Voltage stabilizer | Water sprinkler, Traffic light controller |

**Q3] What are Topologies? Explain the Types of Topologies with Diagram, Advantages and Disadvantages**

**Ans:**

Network topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with each other. Alternately, the network topology may describe how the data is transferred between these nodes. There are two types of network topologies: physical and logical. Physical topology emphasizes the physical layout of the connected devices and nodes, while the logical topology focuses on the pattern of data transfer between network nodes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topology** | **BUS Topology** | **RING Topology** | **STAR Topology** | **MESH Topology** |
| **Definition** | Bus topology is a network type in which every computer and network device is connected to a single cable. When it has exactly two endpoints, then it is called Linear Bus topology. | It is called a ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device. | In this type of topology, all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. | It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has   n(n-1)/2 physical channels to link n devices. |
| **Feature** | * It transmits data only in one direction. * Every device is connected to a single cable | * A number of repeaters are used for Ring topology with a large number of nodes, to prevent data loss repeaters * The transmission is unidirectional. But in Dual Ring Topology, two ring networks are formed, and data flow is in the opposite direction in them. Data is transferred in a sequential manner that is bitten by bit. Data transmitted, has to pass through each node of the network, till the destination node. | * Every node has its own dedicated connection to the hub. * Hub acts as a repeater for data flow. * Can be used with twisted pair, Optical Fiber or coaxial cable. | *Types of Mesh Topology*   * Partial Mesh Topology: In this topology, some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices. * Full Mesh Topology: Each and every nodes or device are connected to each other.   *Features*   * Fully connected. * Robust. * Not flexible. |
| **Advantages** | * It is cost-effective. * Cable required is least compared to another network topology. * Used in small networks. * It is easy to understand. * Easy to expand joining two cables together. | * Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can send data. * Cheap to install and expand | * Fast performance with few nodes and low network traffic. * Hub can be upgraded easily. * Easy to troubleshoot. * Easy to set up and change. * Only that node is affected which has failed, the rest of the nodes can work smoothly. | * Each connection can carry its own data load. * It is robust. * A fault is diagnosed easily. * Provides security and privacy. |
| **Disadvantages** | * Cables fail then the whole network fails. * If network traffic is heavy or nodes are more the performance of the network decreases * Cable has a limited length. * It is slower than the ring topology. | * Troubleshooting is difficult in a ring topology. * Adding or removing the computers disturbs the network activity. * Failure of one computer disturbs the whole network. | * Cost of installation is high. * Expensive to use. * If the hub fails, then the whole network is stopped because all the nodes depend on the hub. * Performance is based on the hub that is it depends on its ability | * Installation and configuration are difficult. * Cabling cost is more. * Bulk wiring is needed. |
| **Diagram** | Image result for bus topology diagram small images | Related image | Related image | Related image |

**Q4.] Differences Between Guided Media and Unguided Media**

**Ans:**

|  |  |  |
| --- | --- | --- |
| **COMPARISON** | **GUIDED MEDIA** | **UNGUIDED MEDIA** |
| **Basic** | The signal requires a physical path for transmission. | The signal is broadcasted through the air or sometimes water. |
| **Alternative name** | It is called wired communication or bounded transmission media. | It is called wireless communication or unbounded transmission media. |
| **Direction** | It supplies direction to signal for travelling. | It does not provide any direction. |
| **Types** | Twisted pair cable, coaxial cable, and fibre optic cable. | Radio wave, microwave and infrared. |

**Q5.]** **Differentiate between connection-oriented and connection-less services.**

**Ans:**

|  |  |
| --- | --- |
| **Connection Oriented Service** | **Connection-less Service** |
| 1. Connection-oriented service is related to the telephone system. | 1. Connection-less service is related to the postal system. |
| 2. Connection-oriented service is preferred by long and steady communication. | 2. Connection-less Service is preferred by busty communication. |
| 3. Connection-oriented service is necessary. | 3. Connection-less Service is not compulsory. |
| 4. Connection-oriented service is feasible. | 4. Connection-less Service is not feasible. |
| 5. In connection-oriented Service, Congestion is not possible. | 5. In connection-oriented Service, Congestion is possible. |
| 6. Connection-oriented service gives the guarantee of reliability. | 6. Connection-less Service does not give the guarantee of reliability. |
| 7. In connection-oriented Service, Packets follow the same route. | 7. In connection-less Service, Packets do not follow the same route. |

**Q6.] What are the steps involved in link-state routing?**

**Ans:**

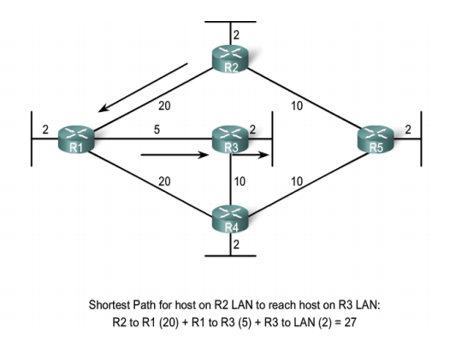
All routers in an OSPF area will complete the following generic link-state routing process to reach a state of convergence:

1. Each router learns about its own links and its own directly connected networks. This is done by detecting that an interface is in the upstate.
2. Each router handles meeting its neighbours on directly connected networks. Link-state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.
3. Each router builds a link-state packet (LSP) holding the state of each directly connected link. This is done by recording all the pertinent information about each neighbour, including neighbour ID, link type, and bandwidth.
4. Each router floods the LSP to all neighbours. Those neighbours store all LSPs received in a database. They then flood the LSPs to their neighbours until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbours in a local database.
5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network. Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to determine the best path to each network.

**Dijkstra’s Algorithm**

All link-state routing protocols apply Dijkstra’s algorithm to calculate the best path route. The algorithm is referred to as the shortest path first (SPF) algorithm. This algorithm uses accumulated costs along each path, from source to destination, to determine the total cost of a route.

In figure below, each path is labelled with an arbitrary value for the cost.

The cost of the shortest path for R2 to send packets to the LAN attached to R3 is 27. Specifically, the cost is R2 to R1 (20) plus R1 to R3 (5) plus R3 to LAN (2). Each router determines its own cost to each destination in the topology. In other words, each router calculates the SPF algorithm and determines the cost from its own perspective.

**Q7.] Explain the contents and requirements of link-state packets.**

**Ans:**

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance-vector routing protocols. Examples of link-state routing protocols include Open Shortest Path First (OSPF) and intermediate system to intermediate system (IS-IS).

The link-state protocol is performed by every switching node in the network (i.e., nodes that are prepared to forward packets; on the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every destination in the network. The collection of best paths will then form the node's routing table.

With link-state routing protocols, a link is an interface on a router. Information about the state of those links is known as link-states.

**Q8.] What is Virtual LAN.**

**Ans:**

* A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs).
* A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.
* VLANs make it easy for network administrators to [partition](https://searchstorage.techtarget.com/definition/partition) a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.
* VLANs are often set up by larger businesses to re-partition devices for better traffic management.
* VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most often.
* VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other.
* VLANs tend to be flexible because they are based on logical connections, rather than physical.
* One or more [network switches](https://searchnetworking.techtarget.com/definition/switch) may support multiple, independent VLANs, creating Layer 2 (data link) implementations of subnets.
* A VLAN is associated with a broadcast domain. It is usually composed of one or more [network switches](https://searchnetworking.techtarget.com/definition/switch).

Types of VLANs include Protocol-based, static, and dynamic VLANs.

* A Protocol VLAN- which has traffic oversaw based on its protocol. A switch will segregate, or forward traffic based on the traffics protocol.
* Static VLAN- also referred to as port-based VLAN, needs a network administrator to assign the ports on a network switch to a virtual network; while:
* Dynamic VLAN- allows a network administrator just to define network membership based on device characteristics, as opposed to switching port location.

Advantages –

* Performance –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to an unnecessary destination. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
* Security – In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs enhance network security.
* Flexibility – VLAN provides flexibility to add, remove the number of hosts we want.
* Cost reduction – VLANs can be used to create broadcast domains which cut the need for expensive routers.

However, a disadvantage of VLANs includes the limitation of 4,096 VLANs per switching domain creates problems for large hosting providers, which often need to distribute tens or hundreds of VLANs for each customer.

**Q9.] What are design issues of OSI layer?**

**Ans:**

# A few design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows:

1. **Reliability**

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

1. **Scalability**

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when modern technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

1. **Addressing**

At a time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can find the sender and receivers of each message.

1. **Error Control**

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods to protect data packets while they are transferred.

1. **Flow Control**

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

1. **Resource Allocation**

Computer networks supply services in the form of network resources to the end-users. The main design issue is to distribute and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is the best usage of the resources.

1. **Statistical Multiplexing**

It is not workable to give a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, to distribute a fraction of the bandwidth or time to each host.

1. **Routing**

There may be multiple paths from the source to the destination. Routing involves choosing the best path among all paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

1. **Security**

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

**Q9.] Brief note on SNMP**

**Ans:**

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used. SNMP is used to manage network devices that span firewalls or embedded devices. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be sorted (and sometimes set) by managing applications

**Simple Network Management Protocol (SNMP) –**  
SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to watch the network, detect network faults, and sometimes even used to configure remote devices.

**SNMP COMPONENTS:**

1. **SNMP Manager –**It is a centralized system used to watch network. It is also known as Network Management Station (NMS)
2. **SNMP agent –**It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. **Management Information Base –**MIB consists of information about resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are variables.

**Q10.] Explain the need for DNS and describe the Protocol?**

**Ans:**

**DNS:**

1. DNS Stands for Domain Name System.
2. DNS is a hierarchical decentralized naming system for computers, services, or any resources connected to the Internet or a private network.
3. DNS is an Internet service that translates domain names into IP addresses.
4. Because domain names are alphabetic, they are easier to remember.
5. The Internet, however, is really based on IP addresses.
6. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.
7. For example, the domain name www.booksmountain.com might translate to 198.105.232.4.

**Need for DNS:**

1. One identifier for a host is its hostname.
2. Hostnames are mnemonic and are therefore appreciated by humans. such as a. www.booksmountain.com. b. www.Facebook.com. c. www.Google.co.in.
3. Hostnames supply little information about the location within the Internet of the host.
4. A hostname such as surf.eurecom.fr, which ends with the country code .fr, tells us that the host is in France, but does not say much more.
5. Furthermore, because hostnames can consist of variable-length alpha-numeric characters, they would be difficult to process by routers.
6. For these reasons, hosts are also found by so-called IP addresses.
7. An IP address consists of four bytes and has a rigid hierarchical structure.
8. An IP address looks like 121.7.106.83, where each period separates one of the bytes expressed in decimal notation from 0 to 127.
9. An IP address is hierarchical because as we scan the address from left to right, we obtain increasingly specific information about where the host is on the Internet. (Like a postal address)
10. An IP address is included in the header of each IP datagram.
11. Internet routers use this IP address to route datagram towards its destination.

**DNS Protocol Functioning:**

1. User type a domain name such as ‘www.booksmountain.com’ into the browser (“client”).
2. The client needs to find the IP address where ‘www. booksmountain.com’ content is located.
3. The browser will send this query to the operating system of the computer.
4. Each operating system is configured to query certain DNS servers (Resolving Name Server).
5. The resolving name server is not aware of the location of ‘Booksmountain.com’, but it does know where the root servers are located.
6. Next, the resolving name server finds the location of the top-level domain name server (In this case COM servers) and sends a query for ‘Booksmountain.com’.
7. Each domain on the Internet has an Authoritative name server.
8. Finally, the authoritative name server will give you the exact IP address of ‘Booksmountain.com’.
9. This information will come back to the resolving name server, which caches the information and sends back the information to your browser.
10. And in the end, you would find yourself on Booksmountain's homepage.
11. All these complex tasks take place in seconds.