UNIT V

OPTICAL NETWORKING :

SONET/SDH Standards, Traffic Engineering: Requirement, Traffic Sizing, Characteristics, Protocols, Time and Delay Considerations, Connectivity, Availability, Reliability and Maintainability and Throughput, Multimedia Over Internet: Transmission, IP Multicasting and VoIP, Domain Name System: Name Space, Domain Name Space, Distribution, Domains, Resolutions and Dynamic Domain Name System, SNMP, Security: IPSec, SSL/TLS, PGP and Firewalls, Datacenter Design and Interconnection Networks.

5.1 Optical Networking

5.1.1 SONET/SDH Standards

Q1. What is SONET/SDH? Write SONET/SDH Transmission Standard. **(Imp.)**

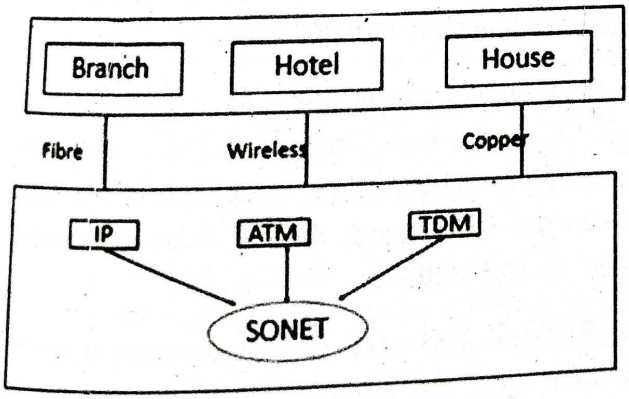
Ans :

SONET stands for synchronous optical network. It offers cost effective transport both in the access area and core of the network.

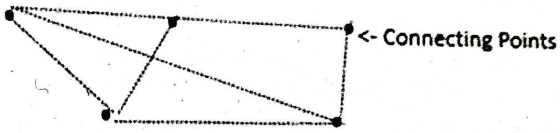
The transport services for the metro are provided by the optical layer. The optical layer has been now giving services for synchronous transmission and performance monitoring.

Example : Telecom Network overview

The SONET/SDH transmission is diagrammatically represented as follows :



Its main role is that if some of the points in a network have not been working properly, the damaged sonnet has the capability to provide alternative points for the transport.



Multiplexing enables the physical medium to carry multiple signals. To place more than one cell on each link, it is some time slot. In SONET, multiplexing is not statistical.

It provides the ability to access traffic at a node without the need for complex packing and unpacking signals.

Hierarchy

The SONET hierarchy is explained below in a stepwise manner :

Step 1:

SONET packages a signal into containers.

Step 2 :

It then adds overhead, so that signal and the quality of transmission are traceable.

Step 3 :

The containers have two names depending on size.

- Virtual Tributary (VT)
- Synchronous Payload Envelope (SPE).

Step 4 :

SONET traffic is packaged in VT and transported in Synchronous signals.

Step 5 :

The SONET line transmission rates are 50, 155, 622 Mbps and 2.5, 10 Gbps.

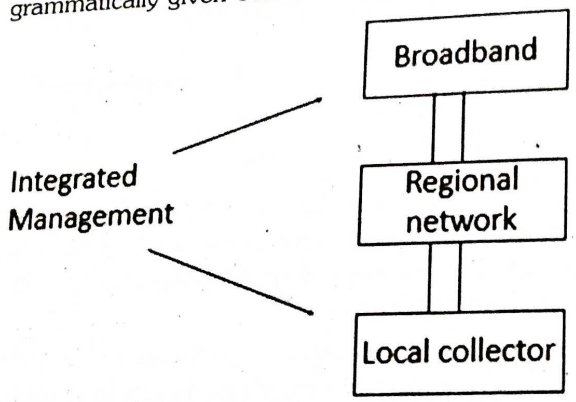
Step 6 :

d SONET is an American National Standards Institution for NA, while synchronous Digital hierarchy (SDH) is for the rest of the world.

Network Architecture of SONET

SONET is not just a simple replacement for SDA but a network in its own configuration, embedded switches and management.

The network architecture of SONET is diagrammatically given below :



Collector rings provide the network interfaces for all access applications. Sometimes, SONET is a multiplexer in customer premises. It checks that the switch processing element is filled to maximum.

Features

The features of SONET are given below :

- Network management
- Protection
- Bandwidth management
- Network simplification
- Mid fibre meet

Benefits

The benefits of SONET are given below :

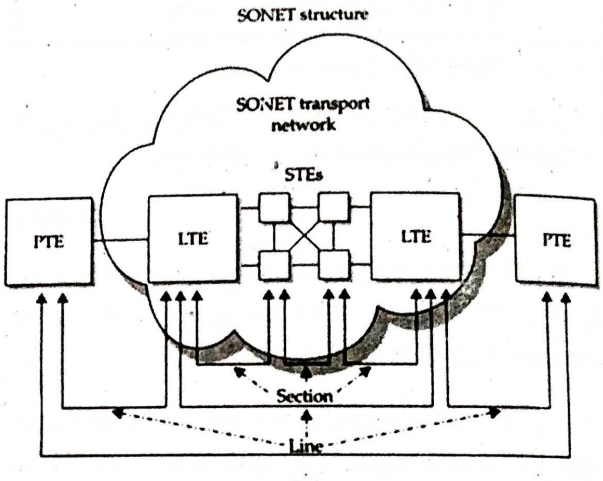
- Increases revenues
- Improved services.
- Reduced operating cost.
- Centralized management.
- Reduced capital investment.

Main Goals

The main goals of SONET are given below :

- Fault tolerance.
- Interoperability among different manufactures.
- Flexibility of upper layer formats.
- Complex monitoring capabilities.

The diagram given below represents the SONET structure :



SONET Structure

SONET Standards

For the line rates ranging up to 10 Gbps (gigabits) per second, we have the SONET standards. So, the line rates of the signals that are approaching the 30 gigabits per second range are possible to deal with SONET protocol.

The optical carrier levels such as level-1, or OC-1. OC-1 are base units of SONET and they support up to 51.84 Mbps (megabytes) per second. On the other hand, the OC-3 level supports the triple bandwidth.

ANSI T1.105 and T1.117 specify the ANSI standards.

Let us look at the speed table of the SONET network.

Electrical Signal	Optical Carrier	Speed
STS-1	OC-1	51.48 Mbps
STS-3	OC-3	155.52 Mbps
STS-12	OC-12	622.08 Mbps
STS-24	OC-24	1.24 Gbps
STS-48	OC-48	2.48 Gbps
STS-192	OC-192	9.95 Gbps

5.2 Traffic Engineering

5.2.1 Requirement

Q2. Explain the requirements of Traffic engineering.

(Imp.)

Ans :

Here are some of the key requirements of traffic engineering in computer networks:

1. **Efficient utilization of network resources:** Traffic engineering is essential to ensure that network resources are used efficiently. By implementing traffic engineering measures, network administrators can ensure that traffic is distributed across the network in a way that maximizes network performance and minimizes congestion and delays.

2. **Quality of service (QoS):** QoS is a key requirement of traffic engineering, as it is essential to ensure that different types of traffic are given appropriate priority on the network. By implementing QoS measures such as traffic shaping, bandwidth reservation, and packet prioritization, network administrators can ensure that critical traffic such as voice and video are given the necessary bandwidth and latency to function effectively.

3. **Fault tolerance:** Fault tolerance is an important requirement of traffic engineering, as it is essential to ensure that the network can continue to function even in the event of device or link failures. By implementing redundancy measures such as link aggregation, backup devices, and alternate routing paths, network administrators can ensure that the network remains operational even during periods of disruption.

4. **Scalability:** Scalability is another important requirement of traffic engineering, as it is essential to ensure that the network can grow and adapt to changing demands over time. By implementing scalable network architectures and protocols, network administrators can ensure that the network can handle increasing traffic volume and bandwidth requirements without compromising performance or reliability.

5. **Security:** Security is a critical requirement of traffic engineering, as it is essential to protect the network from threats such as unauthorized access, data breaches, and denial-of-service attacks. By implementing security measures such as firewalls, intrusion detection and prevention systems, and encryption and authentication mechanisms, network administrators can ensure that the network remains secure and protected from malicious activity.

Overall, the requirements of traffic engineering in computer networks are focused on ensuring that the network is reliable, efficient, and able to meet the needs of its users and customers. By implementing traffic engineering measures that prioritize QoS, fault tolerance, scalability, and security, network administrators can create a network that is optimized for performance, reliability, and user satisfaction.

5.2.2 Traffic Sizing

Q3. What is traffic sizing? Write about it.

(Imp.)

Ans :

Traffic sizing is a critical aspect of traffic engineering, as it involves determining the amount of traffic that will be carried over the network and the capacity that will be required to handle this traffic. Effective traffic sizing is essential to ensure that the network can meet the needs of its users and customers, and can handle increasing traffic volumes over time.

Here are some key considerations when performing traffic sizing in traffic engineering:

1. **Determine the types of traffic:** Before performing traffic sizing, it is important to determine the types of traffic that will be carried over the network. This can involve identify-

ing different traffic classes, such as voice, video, and data, and determining the bandwidth requirements and QoS requirements for each class.

2. **Measure traffic volume:** Once the types of traffic have been identified, the next step is to measure the traffic volume for each traffic class. This can involve using network monitoring and analysis tools to track traffic patterns over time, and to identify peak traffic periods and bandwidth requirements.

3. **Determine capacity requirements:** Based on the traffic volume measurements, the next step is to determine the capacity requirements for the network. This can involve calculating the total bandwidth required to handle all traffic classes, and identifying any bottlenecks or capacity constraints that may need to be addressed.

4. **Plan for growth:** When performing traffic sizing, it is important to plan for future growth and increasing traffic volumes. This can involve estimating future traffic volumes and capacity requirements, and implementing scalable network architectures and protocols that can accommodate increasing traffic volumes over time.

5. **Test and validate:** Once traffic sizing measures have been implemented, it is important to test and validate the network to ensure that it is performing effectively. This can involve using network testing tools to simulate different traffic scenarios and identify any performance or capacity issues that may need to be addressed.

Overall, traffic sizing is a critical aspect of traffic engineering, as it involves determining the amount of traffic that will be carried over the network and the capacity that will be required to handle this traffic. By following these key considerations and implementing effective traffic sizing measures, network administrators can ensure that the network is optimized for performance, reliability, and user satisfaction.

5.2.3 Characteristics

Q4. What are the characteristics of traffic engineering? Write about them.

Ans :

Here are some of the key characteristics of traffic engineering in computer networks:

1. **Optimization:** Traffic engineering is focused on optimizing the performance of a network by managing the flow of data traffic. This involves using various techniques and algorithms to ensure that data is delivered efficiently and reliably to its intended destination.

2. **Dynamic:** Traffic engineering is a dynamic process that requires continuous monitoring and adjustment. Network conditions and traffic patterns can change rapidly, and traffic engineering algorithms must be able to adapt to these changes in real-time.

3. **QoS:** Quality of Service (QoS) is a key aspect of traffic engineering. QoS mechanisms can be used to prioritize certain types of traffic over others, based on factors such as bandwidth requirements, delay sensitivity, and packet loss tolerance.

4. **Load Balancing:** Load balancing is another important aspect of traffic engineering. By distributing traffic across multiple paths or links, load balancing can help prevent bottlenecks and ensure that network resources are utilized evenly.

5. **Resource Optimization:** Traffic engineering is also focused on optimizing the use of network resources. By managing traffic flows and routing paths, traffic engineering can help ensure that network resources are used efficiently and effectively.

6. **Scalability:** Traffic engineering is designed to be scalable, allowing it to handle traffic flows of varying sizes and types. This is essential in today's networks, where traffic patterns can change rapidly and unexpectedly.

Overall, traffic engineering plays a critical role in ensuring the performance and reliability of computer networks. By managing

traffic flows, optimizing network resources, and adapting to changing conditions, traffic engineering helps to ensure that data is delivered quickly and reliably to its intended destination.

5.2.4 Protocols

Q5. Explain about the protocols used in traffic engieneering. **(Imp.)**

Ans :

Here are some of the protocols commonly used in traffic engineering in computer networks:

1. **Multiprotocol Label Switching (MPLS):** MPLS is a protocol used to improve the performance and efficiency of network traffic. It enables routers to forward data packets based on labels rather than IP addresses, allowing for faster and more efficient routing.
2. **Border Gateway Protocol (BGP):** BGP is a protocol used to exchange routing information between different networks. It is commonly used in traffic engineering to help network administrators optimize routing paths and prevent congestion.
3. **Resource Reservation Protocol (RSVP):** RSVP is a protocol used to reserve network resources, such as bandwidth, for specific traffic flows. It is often used in QoS mechanisms to ensure that critical traffic receives the necessary resources to meet performance requirements.
4. **Differentiated Services (DiffServ):** DiffServ is a protocol used to prioritize and classify network traffic based on its importance and characteristics. It enables network administrators to implement QoS mechanisms and ensure that critical traffic receives priority over less important traffic.
5. **Traffic Engineering Extensions to OSPF (OSPF-TE):** OSPF-TE is a protocol extension to OSPF that enables network administrators to optimize routing paths and manage network resources more efficiently. It is commonly used in large-scale networks and in situations where network performance is critical.

Overall, these protocols play a critical role in traffic engineering, enabling network administrators to manage network traffic and resources more effectively and efficiently.

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a protocol used in computer networks to improve the performance and efficiency of network traffic. It works by forwarding data packets based on labels, rather than traditional routing based on IP addresses.

In the context of traffic engineering, MPLS is commonly used to optimize network routing and resource allocation. Here are some of the key aspects of MPLS that are relevant to traffic engineering:

1. **Label Switching:** In MPLS, labels are used to identify the path that a packet should take through the network. This enables routers to forward packets more quickly and efficiently, as they don't need to perform traditional IP routing lookups for each packet.
2. **Traffic Engineering:** MPLS includes traffic engineering capabilities that allow network administrators to optimize network routing and resource allocation. This involves using various algorithms and techniques to adjust the flow of traffic through the network, ensuring that critical traffic receives the necessary resources and that network resources are used efficiently.
3. **Quality of Service (QoS):** MPLS supports Quality of Service (QoS) mechanisms that enable network administrators to prioritize certain types of traffic over others, based on factors such as bandwidth requirements, delay sensitivity, and packet loss tolerance.
4. **Virtual Private Networks (VPNs):** MPLS can be used to create virtual private networks (VPNs), which allow multiple networks to be connected securely over a public network. This is particularly useful for organizations that need to connect multiple locations or remote workers to a central network.

Overall, MPLS is a powerful tool for traffic engineering in computer networks, enabling network administrators to optimize

routing, allocate resources, and prioritize traffic based on its importance and characteristics. By using MPLS, organizations can improve network performance, reliability, and security, and ensure that their critical applications and services are delivered efficiently and reliably.

Traffic Engineering Extensions to OSPF (OSPF-TE):

Traffic Engineering Extensions to OSPF (OSPF-TE) is a protocol extension to the Open Shortest Path First (OSPF) routing protocol, which is commonly used in computer networks. OSPF-TE enables network administrators to optimize network routing and resource allocation, particularly in large-scale networks where traffic engineering is critical.

Here are some of the key aspects of OSPF-TE that are relevant to traffic engineering:

1. **Traffic Engineering Database:** OSPF-TE includes a traffic engineering database that provides detailed information about network topology, link capacity, and other factors that are relevant to traffic engineering. This enables network administrators to make informed decisions about how to route traffic through the network.
2. **Traffic Engineering Extensions:** OSPF-TE includes several extensions to the standard OSPF protocol that are specifically designed for traffic engineering. These extensions enable network administrators to set up traffic engineering tunnels, which are virtual links that can be used to carry traffic between specific points in the network.
3. **Quality of Service (QoS):** OSPF-TE supports Quality of Service (QoS) mechanisms that enable network administrators to prioritize certain types of traffic over others, based on factors such as bandwidth requirements, delay sensitivity, and packet loss tolerance.
4. **Path Computation Element (PCE):** OSPF-TE includes a Path Computation Element (PCE), which is responsible for calculating the optimal path for traffic through the network. The PCE uses traffic engineering data from the traffic engineering database to determine the best path for each traffic flow.
5. **Resource Reservation Protocol (RSVP):** OSPF-TE works in conjunction with the Resource Reservation Protocol (RSVP), which is used to reserve network resources, such as bandwidth, for specific traffic flows. This enables network administrators to ensure that critical traffic receives the necessary resources to meet performance requirements.

Overall, OSPF-TE is a powerful tool for traffic eng\ineering in computer networks, enabling network administrators to optimize routing, allocate resources, and prioritize traffic based on its importance and characteristics. By using OSPF-TE, organizations can improve network performance, reliability, and scalability, and ensure that their critical applications and services are delivered efficiently and reliably.

5.2.5 Time And Delay Considerations

Q6. Write about time and delay considerations of traffic egineeering.

Ans :

Time and delay considerations are critical in traffic engineering, as they can have a significant impact on network performance and user experience. Here are some of the key time and delay considerations in traffic engineering:

1. **Latency:** Latency refers to the time it takes for a data packet to travel from its source to its destination. Latency can be affected by a variety of factors, including the distance between the source and destination, the number of network hops the packet must traverse, and the processing time at each hop. In traffic engineering, minimizing latency is often a key goal, as it can improve the performance of real-time applications such as video conferencing and online gaming.
2. **Jitter:** Jitter refers to the variation in latency between data packets. Jitter can be caused by factors such as network congestion and varying processing times at different network hops. In traffic engineering, minimizing jitter is important to ensure that real-time applications such as voice and video are delivered smoothly and without interruptions.

3. **Packet Loss:** Packet loss occurs when data packets are dropped or lost during transmission. Packet loss can be caused by a variety of factors, including network congestion and errors in the transmission process. In traffic engineering, minimizing packet loss is important to ensure that critical data is not lost or corrupted during transmission.

4. **Quality of Service (QoS):** Quality of Service (QoS) mechanisms are used in traffic engineering to ensure that certain types of traffic receive priority over others. QoS mechanisms can be used to prioritize real-time applications such as voice and video, and to allocate network resources such as bandwidth and buffer space to ensure that critical traffic receives the necessary resources.

5. **Service Level Agreements (SLAs):** Service Level Agreements (SLAs) are contracts between network service providers and their customers that define the level of service that will be provided. SLAs typically include performance metrics such as latency, jitter, and packet loss, and specify the consequences if the agreed-upon levels of service are not met.

Overall, time and delay considerations are critical in traffic engineering, as they can have a significant impact on network performance, user experience, and customer satisfaction. By carefully managing latency, jitter, and packet loss, and implementing QoS mechanisms and SLAs, network administrators can ensure that their networks deliver the necessary performance and reliability to meet the needs of their users and customers.

5.2.6 Connectivity

Q7. How to do connectivity in network traffic engineering? Explain.

Ans : **(Imp.)**

Connectivity is a key consideration in traffic engineering in computer networks, as it is essential to ensure that network devices can communicate with each other reliably and efficiently. Here are some of the key connectivity considerations in traffic engineering:

To ensure effective connectivity in network traffic engineering, there are several steps that network administrators can take:

1. **Define network requirements:** Before implementing connectivity measures, it is important to define the requirements of the network. This can involve determining the types of traffic that will be carried over the network, the number and types of devices that will be connected, and the expected levels of traffic volume and bandwidth.

2. **Design network topology:** Once network requirements have been defined, the next step is to design the network topology. This can involve determining the location of network devices, the types of connections that will be used between devices, and the routing protocols and network protocols that will be implemented.

3. **Implement redundancy:** Redundancy measures can be implemented to ensure that there are multiple paths for traffic to take between devices. This can involve implementing link aggregation, using multiple routing protocols to create alternate paths, and deploying backup devices or failover mechanisms.

4. **Load balance traffic:** Load balancing can be used to distribute traffic evenly across multiple network links or devices. This can involve implementing load balancing algorithms that take into account factors such as link capacity and network congestion, and using technologies such as network virtualization to create multiple virtual networks that can be load balanced independently.

5. **Ensure interoperability:** Interoperability measures can be implemented to ensure that different network devices and protocols can work together effectively. This can involve implementing standardized protocols and interfaces, and ensuring that devices are properly configured and compatible with one another.

6. **Ensure security:** Security measures can be implemented to protect network connectivity from threats such as unauthorized access,

data breaches, and denial-of-service attacks. This can involve implementing firewalls, intrusion detection and prevention systems, and encryption and authentication mechanisms.

7. **Monitor network performance:** Finally, it is important to monitor network performance to ensure that connectivity measures are working effectively. This can involve using network monitoring and analysis tools to track traffic volume, latency, packet loss, and other performance metrics, and using this data to identify areas for improvement and optimize network performance over time.

By following these steps, network administrators can ensure effective connectivity in network traffic engineering, and create a network that is reliable, secure, and able to meet the needs of its users and customers.

5.2.7 Availability

Q8. Write about the availability aspect in traffic engineering.

Ans : **(Imp.)**

Availability is a critical aspect of traffic engineering in computer networks, as it is essential to ensure that the network is always available to meet the needs of its users and customers. Availability measures can be used to ensure that the network is operational and accessible at all times, and to minimize downtime and service interruptions.

Here are some key considerations when implementing availability measures in traffic engineering:

1. **Redundancy:** Redundancy is a critical availability measure that involves implementing backup devices, alternate routing paths, and other redundancy measures to ensure that the network remains operational even in the event of device or link failures. By implementing redundancy measures, network administrators can ensure that critical services and applications remain available even during periods of disruption.

2. **Load balancing:** Load balancing is another important availability measure that involves distributing traffic across multiple network devices or paths to ensure that no single device or link becomes overloaded or congested. By implementing load balancing measures, network administrators can ensure that the network remains responsive and available even during periods of high traffic volume.

3. **Failover:** Failover is an availability measure that involves automatically switching to backup devices or links in the event of a device or link failure. By implementing failover measures, network administrators can ensure that critical services and applications remain available even in the event of a failure.

4. **Service level agreements (SLAs):** Service level agreements are agreements between network administrators and service providers that define the availability and performance guarantees for network services and applications. By implementing SLAs, network administrators can ensure that service providers are held accountable for meeting their availability and performance commitments.

5. **Monitoring and reporting:** Monitoring and reporting are essential availability measures that involve using network monitoring and analysis tools to track network performance and identify potential issues or bottlenecks. By implementing monitoring and reporting measures, network administrators can proactively identify and address potential availability issues before they become critical.

Overall, availability is a critical aspect of traffic engineering in computer networks, as it is essential to ensure that the network remains operational and accessible at all times. By following these key considerations and implementing effective availability measures, network administrators can ensure that the network is optimized for performance, reliability, and user satisfaction.

5.2.8 Reliability And Maintainability and Throughput

Q9. Write about reliability, maintainability and throughput in traffic engineering. **(Imp.)**

Ans :

Reliability

Reliability is a key aspect of traffic engineering in computer networks, as it is essential to ensure that the network can provide dependable and consistent service to its users and customers. Reliability measures can be used to ensure that the network is resilient and can handle unexpected events, and to minimize service disruptions and downtime.

Here are some key considerations when implementing reliability measures in traffic engineering:

1. **Redundancy:** Redundancy is a critical reliability measure that involves implementing backup devices, alternate routing paths, and other redundancy measures to ensure that the network remains operational even in the event of device or link failures. By implementing redundancy measures, network administrators can ensure that critical services and applications remain available and reliable even during periods of disruption.
2. **Fault tolerance:** Fault tolerance is another important reliability measure that involves designing the network to be able to continue functioning even in the event of component failures or other issues. This can involve using redundant components, load balancing, and other measures to ensure that the network can continue to operate even in the face of unexpected events.
3. **Backup and recovery:** Backup and recovery measures are essential reliability measures that involve implementing data backup and recovery procedures to ensure that critical data and applications can be restored in the event of a system failure or other issue. By implementing effective backup and recovery measures, network administrators can ensure that critical data and applications remain available and reliable even in the face of unexpected events.
4. **Monitoring and reporting:** Monitoring and reporting are essential reliability measures that involve using network monitoring and analysis tools to track network performance and identify potential issues or bottlenecks. By implementing monitoring and reporting measures, network administrators can proactively identify and address potential reliability issues before they become critical.
5. **Disaster recovery:** Disaster recovery measures are essential reliability measures that involve implementing plans and procedures to ensure that critical network services and applications can be restored in the event of a major disaster or catastrophic event. By implementing effective disaster recovery measures, network administrators can ensure that critical network services and applications remain available and reliable even in the face of major disruptions.

Maintainability

Maintainability is an important aspect of traffic engineering in computer networks, as it is essential to ensure that the network can be easily managed, updated, and maintained over time. Maintainability measures can be used to ensure that the network remains efficient and up-to-date, and to minimize the cost and effort required to manage and maintain the network.

Here are some key considerations when implementing maintainability measures in traffic engineering:

1. **Modularity:** Modularity is a critical maintainability measure that involves designing the network to be composed of discrete modules or components that can be easily updated or replaced as needed. By implementing modularity measures, network administrators can ensure that the network remains adaptable and can be easily updated to meet changing needs over time.
2. **Standardization:** Standardization is another important maintainability measure that involves using standard protocols and interfaces

to ensure that network components can be easily interchanged and updated as needed. By implementing standardization measures, network administrators can ensure that the network remains interoperable and can be easily updated with new components and technologies.

3. **Configuration management:** Configuration management is an essential maintainability measure that involves implementing procedures for managing network configurations and ensuring that they remain up-to-date and consistent over time. By implementing effective configuration management measures, network administrators can ensure that the network remains optimized and efficient over time.

4. **Documentation:** Documentation is an important maintainability measure that involves creating and maintaining up-to-date documentation of network configurations, procedures, and processes. By implementing effective documentation measures, network administrators can ensure that knowledge and expertise are transferred effectively and that the network remains manageable over time.

5. Training and education: Training and education are essential maintainability measures that involve providing ongoing training and education to network administrators and other personnel to ensure that they have the knowledge and skills needed to manage and maintain the network effectively. By implementing effective training and education measures, network administrators can ensure that the network remains up-to-date and efficient over time.

Throughput

Throughput is an important aspect of traffic engineering in computer networks, as it measures the amount of data that can be transmitted through the network over a given period of time. Optimizing throughput is critical to ensuring that the network can handle the amount of traffic that is generated by users and applications, and that data can be transmitted efficiently and quickly.

Here are some key considerations for optimizing throughput in traffic engineering:

1. **Bandwidth:** Bandwidth is the amount of data that can be transmitted through the network at any given time. By increasing bandwidth, network administrators can improve the network's throughput and ensure that data can be transmitted quickly and efficiently.

2. **Traffic prioritization:** Prioritizing traffic based on its importance can help ensure that critical data is transmitted first, while less important data is transmitted later. By implementing traffic prioritization measures, network administrators can optimize the network's throughput and ensure that the most important data is transmitted quickly and efficiently.

3. **Quality of Service (QoS):** QoS is a measure of the network's ability to provide a consistent level of service to users, even when there is high network traffic. By implementing QoS measures, network administrators can ensure that the network's throughput remains consistent and that data can be transmitted quickly and efficiently.

4. **Load balancing:** Load balancing involves distributing network traffic across multiple network paths to optimize network throughput and prevent congestion. By implementing load balancing measures, network administrators can ensure that the network's throughput remains consistent and that data can be transmitted quickly and efficiently.

5. **Network topology:** The network topology refers to the physical and logical layout of the network. By optimizing the network topology, network administrators can ensure that data can be transmitted quickly and efficiently, and that the network's throughput remains consistent.

5.3 Multimedia Over Internet

5.3.1 Transmission

Q10. Explain about Transmission of multimedia over the internet.

(Imp.)

Ans :

Transmission of multimedia over the internet involves the sending of multimedia content such as audio, video, and images over the internet to one or more recipients. There are several ways in which multimedia can be transmitted over the internet, including:

1. **Streaming:** Streaming involves sending multimedia content over the internet in real-time, allowing the recipient to access the content as it is being transmitted. Streaming can be done using different protocols such as HTTP, RTSP, and RTP.
2. **Downloading:** Downloading involves saving multimedia content onto a recipient's device for later playback. Multimedia content can be downloaded from various sources such as websites, peer-to-peer networks, and cloud storage services.
3. **Uploading:** Uploading involves sending multimedia content from a sender's device to a remote server or other recipient's device. This is commonly done when sharing multimedia content such as videos or images on social media platforms or cloud storage services.
4. **Email attachment:** Multimedia content can be sent over the internet as email attachments. However, email attachment size limitations may restrict the size and quality of the multimedia content that can be sent.

The transmission of multimedia over the internet requires a high-speed and reliable internet connection, as well as appropriate encoding and decoding techniques to ensure the quality and integrity of the content being transmitted. Different multimedia formats may also require specific codecs for efficient transmission over the internet.

There are various transmission protocols used in multimedia to ensure efficient and reliable transmission of audio, video, and other multimedia content over the internet. Some of the commonly used transmission protocols in multimedia are:

1. **Real-time Transport Protocol (RTP):** RTP is a protocol used for real-time transmission of multimedia content, such as audio and video, over the internet. It provides mechanisms for the transmission and reception of multimedia data, as well as QoS control for optimal performance.
2. **User Datagram Protocol (UDP):** UDP is a connectionless protocol that is commonly used in multimedia streaming applications for fast and efficient transmission of audio and video content. It does not provide reliability or error control, but is suitable for real-time applications where some data loss can be tolerated.
3. **Transmission Control Protocol (TCP):** TCP is a reliable, connection-oriented protocol that is commonly used for multimedia content transmission, such as file downloads and email attachments. It ensures reliable delivery of data by providing error checking, retransmission of lost packets, and flow control.
4. **HTTP Live Streaming (HLS):** HLS is a protocol used for streaming multimedia content over the internet, typically used in applications such as video-on-demand and live streaming. It segments multimedia content into smaller chunks, which are then delivered over HTTP using standard web servers.
5. **Dynamic Adaptive Streaming over HTTP (DASH):** DASH is another streaming protocol used for adaptive streaming of multimedia content. It allows the sender to dynamically adjust the quality of the content based on the recipient's network conditions, providing a better streaming experience.

5.3.2 Ip Multicasting And Voip

Q11. What is IP multicasting and Voice Over internet protocol.

Ans : **(Imp.)**

IP multicasting and VoIP (Voice over Internet Protocol) are two technologies that play a critical role in multimedia transmission over the internet.

IP multicasting is a technique for sending data from one sender to multiple recipients over a network. It is particularly useful for streaming multimedia content, such as live video or audio, to a large number of users simultaneously. With IP multicasting, the sender only needs to send a single copy of the data, and the network takes care of replicating the data and delivering it to all the intended recipients. This reduces network congestion and ensures efficient use of network resources.

VoIP, on the other hand, is a technology that allows voice communications over the internet. It converts analog voice signals into digital data packets, which can be transmitted over the internet using IP networks. VoIP is an efficient and cost-effective way of making voice calls, especially over long distances. With VoIP, users can make calls from any device connected to the internet, including smartphones, tablets, and laptops.

When used together, IP multicasting and VoIP can enhance the quality and efficiency of multimedia transmissions over the internet. For example, a VoIP conference call can be multicast to multiple participants, reducing the amount of network traffic and improving call quality. Additionally, IP multicasting can be used to distribute multimedia content to remote offices or users, enabling efficient and cost-effective distribution of information.

However, implementing IP multicasting and VoIP requires careful planning and configuration of network infrastructure to ensure optimal performance and minimize network congestion. Appropriate QoS mechanisms must also be employed to ensure the timely and reliable delivery of multimedia data packets over the network.

5.3.3 Domain Name System

5.3.4 Name Space

Q12. What is Namespace? Explain.

Ans :

Namespace is the abstract space or collection of all possible addresses, names, or identifiers of objects on a network, internetwork, or the Internet. A namespace is "the space of all names" for a given type of network name.

A simple example of a namespace is an IP address space, which consists of the space of all possible IP addresses. This space is divided into class A, class B, and so on, which represent disjoint subgroups of the IP address space. Generally, every node on a TCP/IP network, internetwork, or the Internet must occupy a unique point in the IP address space that is, it must have a unique IP address. This ensures that a packet directed to a particular node (such as a computer, network printer, or router interface) can be addressed with the IP address of that node. If two nodes on a network were to have the same IP address number, a packet intended for one might end up at the other. The exception is when you have a private network connected to the Internet through a firewall that uses network address translation (NAT) or some other scheme to hide the addresses of nodes in the private network from the Internet. In this case, if no direct communication is expected between nodes in the two networks (except through the firewall), nodes in the private network can be assigned arbitrary IP addresses such as 10.x.y.z. Another common example of a namespace is the DNS namespace of the Internet. Unlike the space of IPv4 addresses just described, the DNS namespace is hierarchical in structure and arbitrarily scalable (except so far as a node in DNS namespace must generally map to some specific IP address). It also has the advantage of being a logical. naming scheme, in contrast to a physical naming scheme such as IP addresses, which are bound to the particular network structure being used

5.3.5 Domain Name Space

Q13. Write about Domain Name Space. (Imp.)

Ans :

The domain names must be very unique and appropriate. The names should be selected from a names pace. The name space can be organized in two ways

(i) Flat name space

(ii) Hierarchical name space

(i) Flat name space

Flat name space is where the name is assigned to the IP address. They do not have any specific structure. In this flat name space, some meaningful names are given to IP address for accessing. The major disadvantage of flat name space is that they cannot be used in large system. Because they need to be accessed and controlled centrally to avoid ambiguity and redundancy. But it is difficult in flat name system. To avoid this major disadvantage hierarchical name space is used in large.

(ii) Hierarchical name space

Hierarchical name space is where the name is made up of several parts. The first part may represent the nature of organization, the second part may represent the name of organization, and third part may represent the department of the organization and so on. In this way the power to control the name space can be decentralized.

Domain Name Space

Domain name space was designed to achieve hierarchical name space. In this, the names are represented as a tree like structure with root element on the top and this tree can have a maximum of 128 levels starting from root element taking the level 0 to level 127.

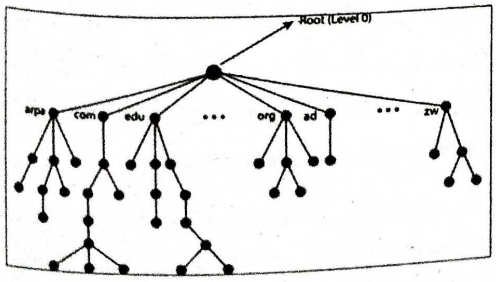


Fig.: Domain Name Space

Figure, represent the domain name space where the root element is present at the top most level i.e., level 0. The root element always represents the NULL string (empty string). The next level to the root element is node (children of root element). Each node in the tree has a label and a domain name.

Label

It is a string which can have maximum of 63 characters. Each node in that level should have different labels thereby assuring the individuality of the domain name.

In other words, Labels are the names given to domains. Domain is a sub tree in domain name space tree structure. The domain can be further divided into sub domains.

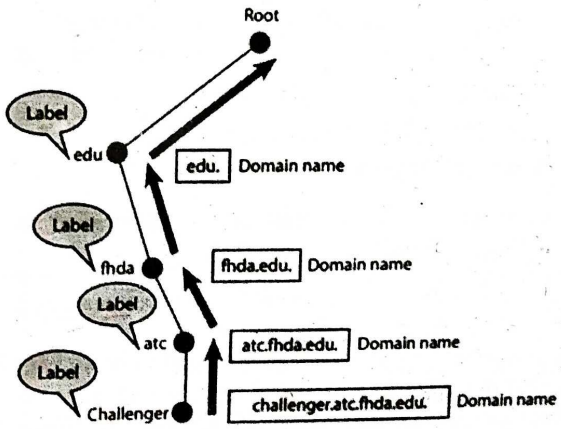


Fig.: Domain Name and Label

Figure, explain the domain name and label clearly. challenger.atc. fhda.edu.is the domain name which is obtained by reading the labels from bottom to top, separating each label by dot (.) Refer Figure.

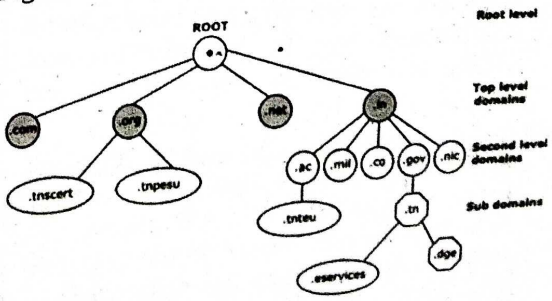


Fig.: Domain representation of www.tnscert.org

Domain name

It is the sequence of labels. In domain name the sequence of labels are separated by dot (.). The domain name is always read from the lower level to higher level i.e., from the leaf node to root node. Since the root node always represent NULL string, all the domain name end with dot.

Basic rules of Domain names

- Domain can consists of Alphabets a through z, and the digits 0 through 9.
- Hyphens are allowed, but hyphens can not be used as first character of a domain name.
- Spaces are not allowed
- Special symbols (such as !, $, &, _ and so on) are not permitted.
- Domain names have the minimum length of 2, and the maximum length of 63 characters. The entire name may be at most 253 characters long.

5.3.6 Distribution

Q14. How domain names are distributed in DNS ? Explain.

Ans :

(Imp.)

Domain names in DNS are organized in a hierarchical structure that starts at the root and extends through various levels of subdomains. Each domain name in the hierarchy is unique and corresponds to a specific IP address or set of IP addresses.

Here's an example of how domain names are distributed in DNS:

1. **Root-Level:** The root level of the DNS hierarchy is represented by a single dot (.), which represents the root zone. This zone contains information about the top-level domains (TLDs) such as .com, .org, .net, .edu, etc. Example: "."
2. **Top-Level Domains (TLDs):** The TLDs are the first level of domains below the root level. There are two types of TLDs: generic top-level domains (gTLDs) and country code top-level domains (ccTLDs). Examples of gTLDs are ".com", ".org", ".net", ".edu", ".gov", and ".info". Examples of ccTLDs are ".us" (United States), ".ca" (Canada), ".uk" (United Kingdom), and ".au" (Australia). Example: ".com"
3. **Second-Level Domains (SLDs):** The second level of domains is below the TLDs and is typically used to identify specific organizations or entities. Example: "google.com", "amazon.com", "wikipedia.org"
4. **Subdomains:** Subdomains are domains that are part of a larger domain. They are created by adding a label to the beginning of an existing domain name, separated by a dot. Examples of subdomains are "mail.google.com", "aws.amazon.com", and "en.wikipedia.org".
5. **Hostnames:** Hostnames are the individual computers or devices that are part of a domain. They are typically identified by a name or IP address. Example: "www.google.com", "mail.amazon.com", "en.wikipedia.org".

Domain names are not case-sensitive. (It may be upper, lower or mixing of both case letters)

Generic Top-Level Domain names:

Top level domain is the last part of a domain name. Generic top level domains are used for generic purpose and maintained by IANA.

Domain Name	Meaning
com	Commercial Organisation
edu	Educational Institutions
gov	Government (US)
mil	Military groups
org	Non profit Organization
net	Networking organization
info	Information serviceproviders

Country top-level domain names

Country domain uses 2-character country abbreviation according to country. For e.g., google.in – for INDIA, google.us for US.

Table 12.2 Country domain names

Domain Name	Meaning
in	India
us	United States
fr	France
uk	United Kingdom
ca	Canada
au	Australia
lk	Srilanka
bd	Bangladesh
cn	China
pk	Pakistan
jP	Japan
sg	Singapore

5.3.7 Domains

Q15. What are domains in DNS? Explain.

Ans :

In DNS (Domain Name System), a domain refers to a unique name that identifies a specific website, network, or organization on the Internet. Domains are used to provide a human-reaclable name that corresponds to the IP address of a resource on the Internet.

Domains are organized in a hierarchical structure, with each level separated by a dot (.) in the domain name. The top-level domains (TLDs) are the highest level of domains and are managed by designated organizations. Examples of TLDs include .com, .org, .net, .gov, .edu, and .info.

Below the TLDs, there are second-level domains (SLDs), which are registered by individuals or organizations and provide a more specific identifier for a website or organization. For example, in the domain name "example.com", "example" is the SLD.

Subdomains are domains that are part of a larger domain and are used to further specify the location of a resource on the Internet. They are created by adding a label to the beginning of an existing domain name, separated by a dot. For example, in the domain name "mail.example.com", "mail" is a subdomain of "example.com".

Overall, domains in DNS provide a way to organize and identify resources on the Internet in a human-readable way. They play a crucial role in the functioning of the Internet by allowing users to access websites and other resources using easy-to-remember domain names rather than IP addresses.

5.3.8 Resolutions And Dynamic Domain Name System

Q16. Write about resolutions in DNS.

Ans : **(Imp.)**

Resolutions

In DNS (Domain Name System), resolution refers to the process of translating a domain name into an IP address. When a user types a domain name into a web browser or other application, the DNS resolution process is initiated to translate the domain name into an IP address that can be used to locate the desired resource on the Internet.

DNS resolution occurs in several steps:

1. **Local DNS resolution:** The first step in the resolution process is to check the local DNS cache on the user's device to see if the domain name has been previously resolved. If the domain name is found in the cache, the associated IP address is used to locate the resource on the Internet.
2. **Recursive DNS resolution:** If the domain name is not found in the local DNS cache, the user's device sends a request to a recursive DNS resolver. The recursive resolver checks its own cache to see if the domain name has been previously resolved. If not, it sends a request to the authoritative DNS server for the domain.
3. **Authoritative DNS resolution:** The authoritative DNS server for the domain receives the request from the recursive resolver and returns the IP address associated with the domain name.
4. **Response and caching:** The recursive resolver receives the IP address from the authoritative DNS server and returns it to the

user's device. The IP address is also cached in the recursive resolver's cache and the local DNS cache on the user's device for future use.

Q17. Explain dynamic domain name system with examples.

Ans :

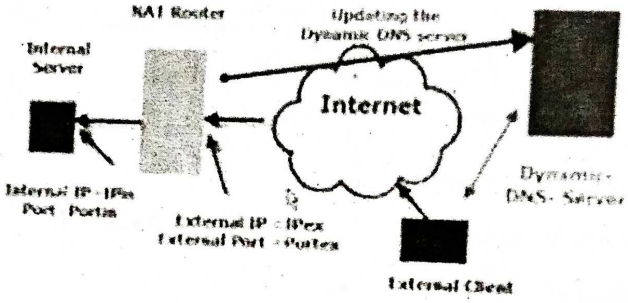
Dynamic DNS (DDNS) is a system that allows a domain name to be automatically updated with the current IP address of a device connected to the Internet, allowing users to easily access the device using a domain name instead of a static IP address.

Here's how dynamic DNS works:

1. **Client software:** A client software is installed on the device that needs to be accessed using a domain name. This could be a web server, file server, or any other device that requires remote access.
2. **Dynamic DNS service:** The client software communicates with a dynamic DNS service provider, such as DynDNS, No-IP, or DuckDNS, to register a domain name and update the IP address associated with the domain name whenever it changes.
3. **IP address changes:** Whenever the device's IP address changes (e.g., due to a change in the Internet Service Provider or a change in the network configuration), the client software communicates with the dynamic DNS service provider to update the IP address associated with the domain name.
4. **Domain name resolution:** When a user wants to access the device, they enter the domain name into a web browser or other application. The DNS resolver queries the dynamic DNS service provider to obtain the current IP address associated with the domain name, allowing the user to connect to the device using the domain name.

Here's an example of how dynamic DNS can be used:

Suppose you have a home security camera that you want to access remotely using a domain name. You install a dynamic DNS client on the camera and register a domain name with a dynamic DNS service provider. Whenever the camera's IP address changes (e.g., due to a change in the ISP or network configuration), the dynamic DNS client updates the IP address associated with the domain name. When you want to access the camera remotely, you enter the domain name into a web browser or other application, and the DNS resolver queries the dynamic DNS service provider to obtain the current IP address associated with the domain name, allowing you to connect to the camera using the domain name.



Here is a textual representation of how DDNS works:

1. The client device with a changing IP address, such as a home security camera, has a DDNS client software installed.
2. The DDNS client communicates with a DDNS service provider to register a domain name and update the IP address associated with the domain name whenever it changes.
3. When the client device's IP address changes, the DDNS client updates the IP address associated with the domain name with the DDNS service provider.
4. When a user wants to access the client device using the domain name, the DNS resolver queries the DDNS service provider to obtain the current IP address associated with the domain name.
5. The DNS resolver returns the current IP address to the user's device, allowing the user to connect to the client device using the domain name.

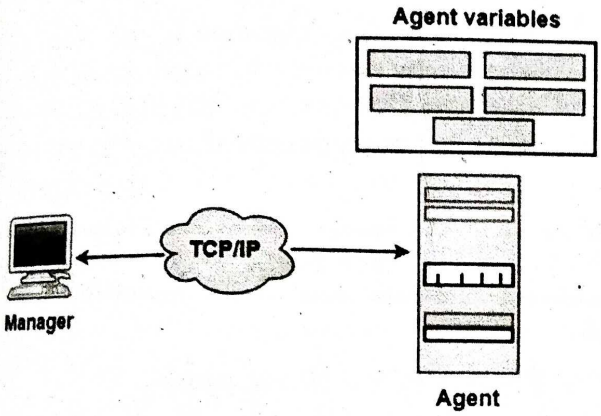
5.3.9 SNMP

Q18. Explain about SNMP Protocol.

Ans :

- SNMP stands for Simple Network Management Protocol.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

SNMP Concept



- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

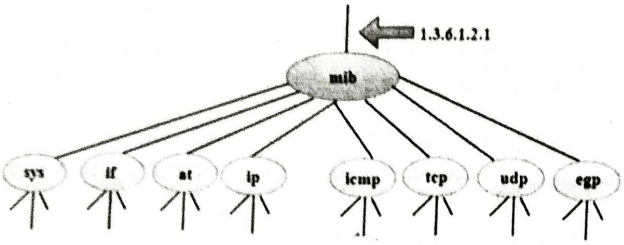
- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

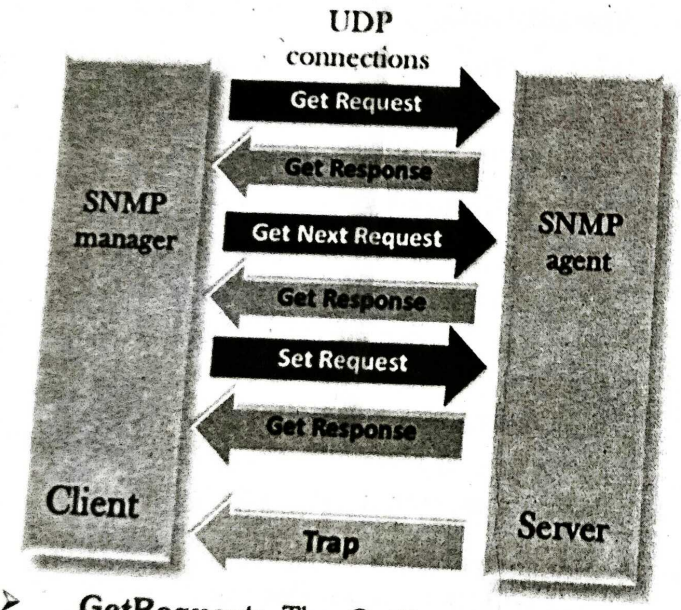
MIB

- The MIB (Management information base) is a second component for the network management.
- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.



SNMP

SNMP defines five types of messages: Get Request, Get Next Request, Set Request, Get Response, and Trap.



- **GetRequest:** The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.
- **GetNextRequest:** The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.
- **GetResponse:** The GetResponse message is sent from an agent to the manager in response to the GetRequest and Get Next Request message. This message contains the value of a variable requested by the manager.
- **SetRequest:** The SetRequest message is sent from a manager to the agent to set a value in a variable.
- **Trap:** The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

5.4 Security

5.4.1 IPSEC

Q19. Explain about IPSec protocol.

Ans : **(Imp.)**

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

Components of IP Security

It has the following components:

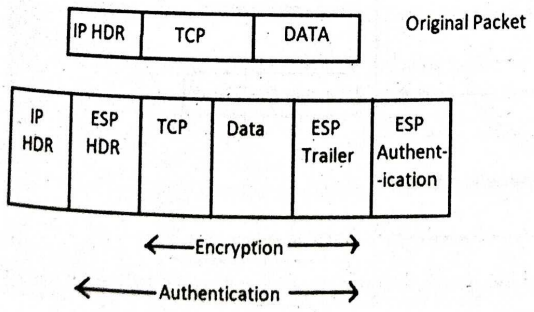
1. **Encapsulating Security Payload (ESP):** It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

2. **Authentication Header (AH) :** It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

IP HDR	AH	TCP	DATA

3. **Internet Key Exchange (IKE):** It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.

2. Then the IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.

3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.

5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.

6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

5.4.2 SSL / TLS

Q20. Write about SSL/TLS? Explain how to establish connection in SSL.

Ans :

SSL (Secure Sockets Layer) is a protocol used to provide secure communication over the internet. It is now commonly referred to as its successor protocol, TLS (Transport Layer Security), but the term SSL is still used colloquially to refer to this type of secure communication.

SSL works by encrypting the data exchanged between two parties, such as a web browser and a

web server, to prevent it from being intercepted and read by unauthorized parties. The SSL protocol establishes a secure connection between the two parties, allowing them to exchange data in a secure and private manner.

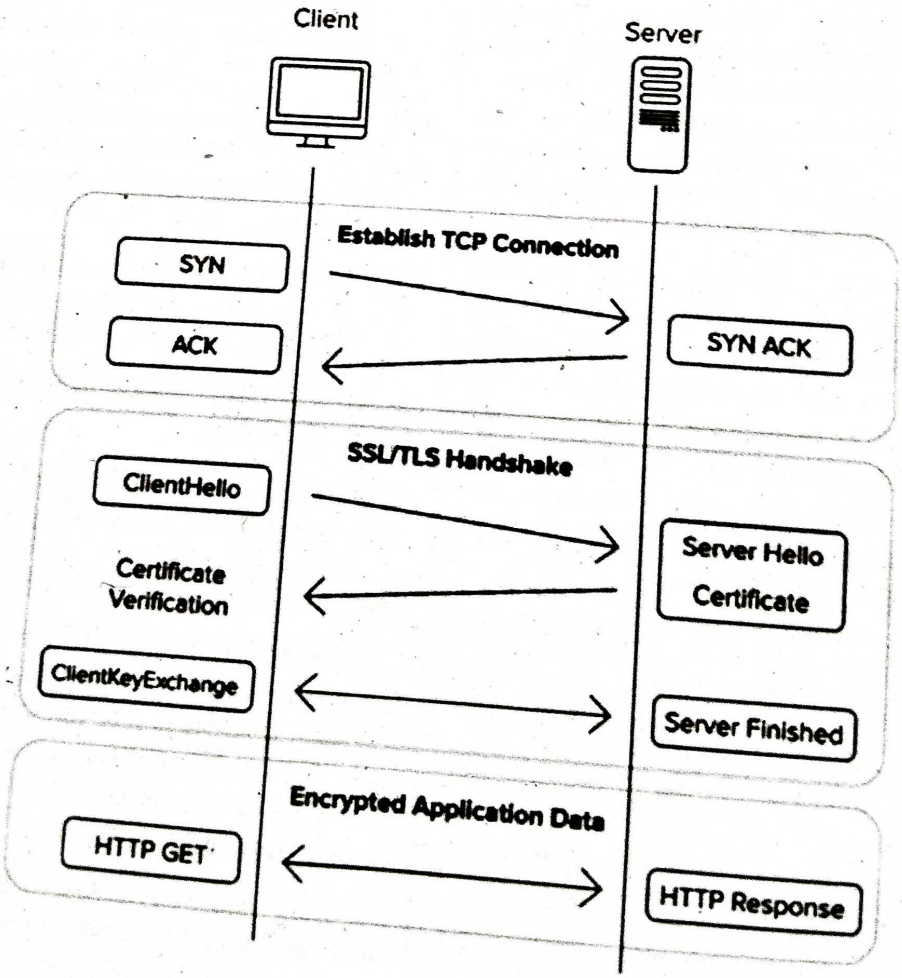
Here are the basic steps involved in an SSL connection:

1. **Handshake:** The SSL handshake is the first step in establishing a secure connection. During the handshake, the client and server exchange information about the SSL/TLS version they support, agree on a cipher suite to use for encryption, and exchange SSL certificates to authenticate each other.
2. **Key exchange:** Once the SSL handshake is complete, the client and server exchange encryption keys to establish a secure session key that will be used to encrypt and decrypt data during the session.
3. **Data exchange:** Once the secure session key has been established, data can be exchanged between the client and server using symmetric encryption. This means that the same key is used to both encrypt and decrypt the data, providing a high level of security.
4. **Session termination:** When the session is complete, the client and server may choose to terminate the SSL connection.

Establishing a SSL/TLS Session

SSL/TLS Handshake

The SSL/TLS handshake takes place once a TCP connection is established.



Here are the basic steps involved in an SSL/TLS handshake:

1. **Client Hello:** The client sends a message to the server containing the SSL/TLS version number, a random number, and a list of cipher suites that it supports.
2. **Server Hello:** The server responds to the client's message with its own SSL/TLS version number, a random number, and the cipher suite that will be used for encryption.
3. **Server Certificate:** The server sends its SSL/TLS certificate to the client, which contains the public key used for encryption.
4. **Client Key Exchange:** The client sends a message to the server containing a pre-master secret, which is used to generate the session key used for encryption.
5. **Server Key Exchange:** If the server requires the client to authenticate itself, it may send a message to the client containing its own pre-master secret.
6. **Server Hello Done:** The server sends a message to the client indicating that the server's part of the handshake is complete.
7. **Client Certificate (optional):** If the server requires client authentication, the client sends its SSL/TLS certificate to the server.
8. **Client Key Exchange:** The client generates the session key using the pre-master secret and sends a message to the server containing the encrypted session key.
9. **Handshake Complete:** The client sends a message to the server indicating that the handshake is complete and that it is ready to begin the encrypted session.

5.4.3 PGP and Firewalls

Q21. Explain PGP protocol.

Ans : **(Imp.)**

PGP

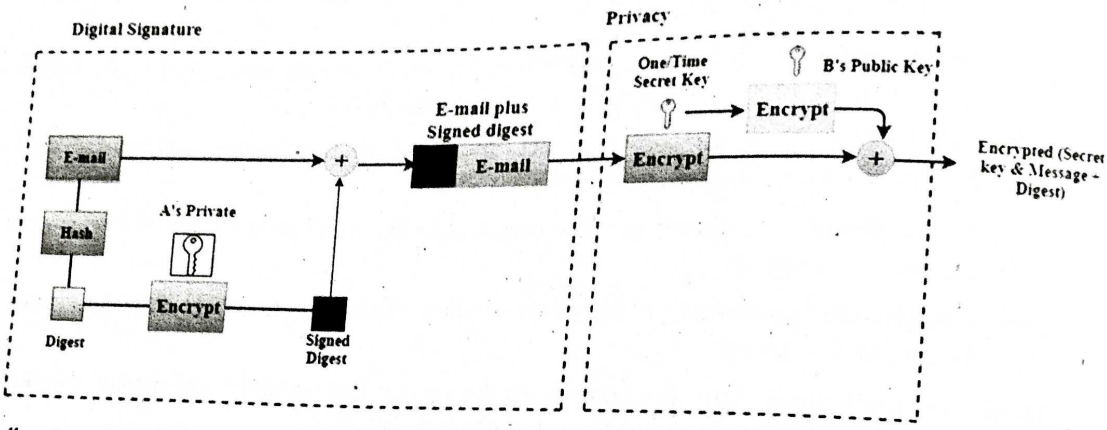
- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.

- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

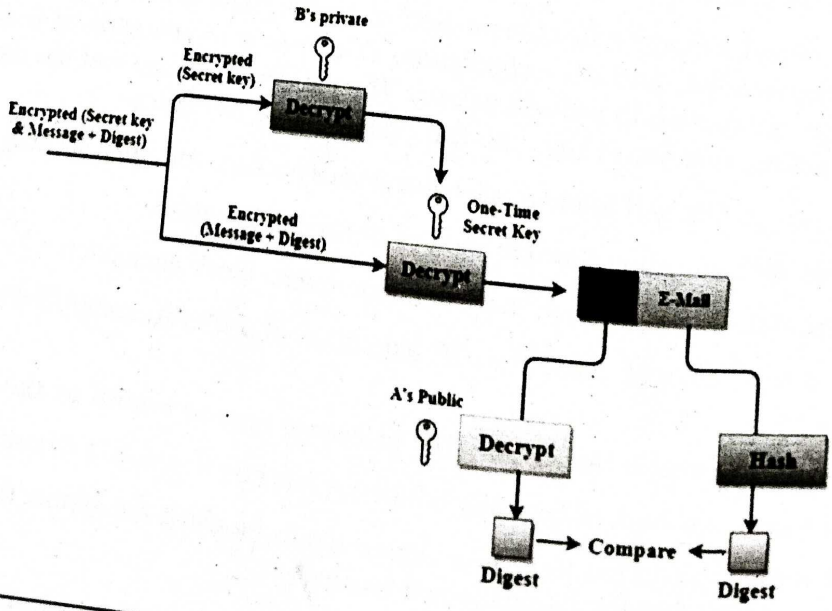
PGP at the Sender site (A)



Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



Disadvantages of PGP Encryption

(i) **The Administration is difficult:** The different versions of PGP complicate the administration.

(ii) **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.

(iii) **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.

(iv) **No Recovery:** Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

Q22. What are firewalls ? explain about them. **(Imp.)**

Ans :

Meaning

A firewall is a network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls are commonly used in internetworking to protect private networks from unauthorized access, viruses, and other malicious activity from the internet.

Firewalls can be implemented at different layers of the networking stack, including:

1. **Network layer:** Firewalls implemented at this layer, such as packet-filtering firewalls, examine incoming and outgoing network packets and filter them based on predetermined rules. These firewalls can block or allow packets based on IP addresses, protocols, ports, and other network-level attributes.
2. **Transport layer:** Firewalls implemented at this layer, such as stateful firewalls, examine the transport layer protocols, such as TCP or UDP, and maintain a state table of ongoing connections. These firewalls can block or allow traffic based on the state of the connection, such as whether it is established or not.
3. **Application layer:** Firewalls implemented at this layer, such as proxy firewalls, examine the contents of application-layer protocols, such as HTTP or FTP, and can block or allow traffic based on the contents of the packets.

Firewalls can also be implemented in different ways, including hardware firewalls and software firewalls. Hardware firewalls are standalone devices that are placed between the private network and the internet, while software firewalls are installed on individual devices, such as servers or desktop computers.

A firewall works by examining network traffic and enforcing predetermined security rules to block or allow traffic based on various criteria. Here's how a firewall works:

1. **Traffic arrives at the firewall:** All traffic entering or exiting the network passes through the firewall.
2. **Firewall examines traffic:** The firewall examines each packet of traffic to determine if it should be allowed through.
3. **Traffic is blocked or allowed:** If the traffic matches the predetermined security rules, it is allowed through the firewall. If it does not match the rules, it is blocked.
4. **Firewall logs traffic:** The firewall logs all traffic that passes through it, which can be used for auditing and troubleshooting purposes.

There are different types of firewalls, including :

1. **Packet filtering firewalls:** Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model and examine the head-

ers of network packets to determine whether they should be allowed through the firewall. This type of firewall can be configured to allow or block traffic based on IP addresses, protocols, and ports.

2. **Stateful firewalls:** Stateful firewalls operate at the transport layer (Layer 4) of the OSI model and maintain a record of ongoing connections. This type of firewall can determine whether incoming packets are part of an established connection or not, and can block or allow traffic based on the state of the connection.

3. **Application-level gateways:** Application-level gateways operate at the application layer (Layer 7) of the OSI model and are also known as proxy firewalls. This type of firewall inspects the contents of application-level protocols, such as HTTP or FTP, and can block or allow traffic based on the contents of the packets.

4. **Next-generation firewalls:** Next-generation firewalls combine traditional firewall functionality with additional security features, such as intrusion prevention, antivirus, and content filtering. They operate at multiple layers of the OSI model and can block or allow traffic based on more advanced criteria, such as user identity or application behavior.

5.4.4 Datacentre Design And Interconnection Networks

Q23. Explain about data center design and interconnection networks.

Ans : **(Imp.)**

Data center design and interconnection networks refer to the physical and logical infrastructure that supports the storage, processing, and transmission of data in a data center. Here are some key aspects of data center design and interconnection networks :

1. Location and size: Data centers are typically located in secure, centralized locations with ample space for servers, storage devices, and networking equipment. They can range in size from small server rooms to large, multi-story buildings.

2. Power and cooling: Data centers require a lot of power to run and cool the equipment. They typically have backup power systems, such as generators or batteries, to ensure uptime during power outages. They also have sophisticated cooling systems to manage the heat generated by the equipment.

3. Physical security: Data centers must be physically secure to protect against theft, vandalism, and other security threats. They often have multiple layers of physical security, such as security guards, biometric authentication, and video surveillance.

4. Networking equipment: Data centers require networking equipment to connect servers and storage devices to each other and to the outside world. This can include routers, switches, firewalls, and load balancers.

5. Interconnection networks: Interconnection networks refer to the physical and logical pathways that connect data centers to each other and to the internet. They can include private networks, such as MPLS or VPNs, and public networks, such as the internet.

6. Cloud computing: Many data centers are now used for cloud computing, which involves providing on-demand access to shared computing resources over the internet. Cloud computing can be provided through public cloud services, such as Amazon Web Services or Microsoft Azure, or through private cloud services, such as Open Stack (or) VM ware.

Overall, data center design and interconnection networks are critical to the functioning of modern businesses and organizations, providing the infrastructure necessary for storing, processing, and transmitting large amounts of data.

Short Question and Answers

1. SONET/SDH.

Ans :

SONET stands for synchronous optical network. It offers cost effective transport both in the access area and core of the network.

The transport services for the metro are provided by the optical layer. The optical layer has been now giving services for synchronous transmission and performance monitoring.

Example : Telecom Network overview

2. Traffic engineering.

Ans :

Here are some of the key requirements of traffic engineering in computer networks:

(i) **Efficient utilization of network resources:** Traffic engineering is essential to ensure that network resources are used efficiently. By implementing traffic engineering measures, network administrators can ensure that traffic is distributed across the network in a way that maximizes network performance and minimizes congestion and delays.

(ii) **Quality of service (QoS):** QoS is a key requirement of traffic engineering, as it is essential to ensure that different types of traffic are given appropriate priority on the network. By implementing QoS measures such as traffic shaping, bandwidth reservation, and packet prioritization, network administrators can ensure that critical traffic such as voice and video are given the necessary bandwidth and latency to function effectively.

(iii) **Fault tolerance:** Fault tolerance is an important requirement of traffic engineering, as it is essential to ensure that the network can continue to function even in the event of device or link failures. By implementing redundancy measures such as link aggregation, backup devices, and alternate routing paths, network administrators can ensure that the network remains operational even during periods of disruption.

3. Traffic Sizing.

Ans :

Traffic sizing is a critical aspect of traffic engineering, as it involves determining the amount of traffic that will be carried over the network and the capacity that will be required to handle this traffic. Effective traffic sizing is essential to ensure that the network can meet the needs of its users and customers, and can handle increasing traffic volumes over time.

4. Characteristics of traffic engineering.

Ans :

(i) **Optimization:** Traffic engineering is focused on optimizing the performance of a network by managing the flow of data traffic. This involves using various techniques and algorithms to ensure that data is delivered efficiently and reliably to its intended destination.

(ii) **Dynamic:** Traffic engineering is a dynamic process that requires continuous monitoring and adjustment. Network conditions and traffic patterns can change rapidly, and traffic engineering algorithms must be able to adapt to these changes in real-time.

(iii) **QoS:** Quality of Service (QoS) is a key aspect of traffic engineering. QoS mechanisms can be used to prioritize certain types of traffic over others, based on factors such as bandwidth requirements, delay sensitivity, and packet loss tolerance.

(iv) **Load Balancing:** Load balancing is another important aspect of traffic engineering. By distributing traffic across multiple paths or links, load balancing can help prevent bottlenecks and ensure that network resources are utilized evenly.

(v) **Resource Optimization:** Traffic engineering is also focused on optimizing the use of network resources. By managing traffic flows and routing paths, traffic engineering can help ensure that network resources are used efficiently and effectively.

5. Protocols used in traffic engieneering.

Ans :

Here are some of the protocols commonly used in traffic engineering in computer networks:

(i) **Multiprotocol Label Switching (MPLS):** MPLS is a protocol used to improve the performance and efficiency of network traffic. It enables routers to forward data packets based on labels rather than IP addresses, allowing for faster and more efficient routing.

(ii) **Border Gateway Protocol (BGP):** BGP is a protocol used to exchange routing information between different networks. It is commonly used in traffic engineering to help network administrators optimize routing paths and prevent congestion.

(iii) **Resource Reservation Protocol (RSVP):** RSVP is a protocol used to reserve network resources, such as bandwidth, for specific traffic flows. It is often used in QoS mechanisms to ensure that critical traffic receives the necessary resources to meet performance requirements.

(iv) **Differentiated Services (DiffServ):** DiffServ is a protocol used to prioritize and classify network traffic based on its importance and characteristics. It enables network administrators to implement QoS mechanisms and ensure that critical traffic receives priority over less important traffic.

6. Multiprotocol Label Switching.

Ans :

Multiprotocol Label Switching (MPLS) is a protocol used in computer networks to improve the performance and efficiency of network traffic. It works by forwarding data packets based on labels, rather than traditional routing based on IP addresses.

In the context of traffic engineering, MPLS is commonly used to optimize network routing and resource allocation.

7. How to do connectivity in network traffic engineering?

Ans :

Connectivity is a key consideration in traffic engineering in computer networks, as it is essential to ensure that network devices can communicate with each other reliably and efficiently. Here are some of the key connectivity considerations in traffic engineering:

To ensure effective connectivity in network traffic engineering, there are several steps that network administrators can take:

(i) **Define network requirements:** Before implementing connectivity measures, it is important to define the requirements of the network. This can involve determining the types of traffic that will be carried over the network, the number and types of devices that will be connected, and the expected levels of traffic volume and bandwidth.

(ii) **Design network topology:** Once network requirements have been defined, the next step is to design the network topology. This can involve determining the location of network devices, the types of connections that will be used between devices, and the routing protocols and network protocols that will be implemented.

(iii) **Implement redundancy:** Redundancy measures can be implemented to ensure that there are multiple paths for traffic to take between devices. This can involve implementing link aggregation, using multiple routing protocols to create alternate paths, and deploying backup devices or failover mechanisms.

8. Reliability.

Ans :

Reliability is a key aspect of traffic engineering in computer networks, as it is essential to ensure that the network can provide dependable and consistent service to its users and customers. Reliability measures can be used to ensure that the network is resilient and can handle unexpected events, and to minimize service disruptions and downtime.

9. Maintainbility.

Ans :

Maintainability is an important aspect of traffic engineering in computer networks, as it is essential to ensure that the network can be easily managed, updated, and maintained over time. Maintainability measures can be used to ensure that the network remains efficient and up-to-date, and to minimize the cost and effort required to manage and maintain the network.

10. Namespace.

Ans :

Namespace is the abstract space or collection of all possible addresses, names, or identifiers of objects on a network, internetwork, or the Internet. A namespace is "the space of all names" for a given type of network name.

A simple example of a namespace is an IP address space, which consists of the space of all possible IP addresses. This space is divided into class A, class B, and so on, which represent disjoint subgroups of the IP address space. Generally, every node on a TCP/IP network, internetwork, or the Internet must occupy a unique point in the IP address space that is, it must have a unique IP address.

11. Domain Name Space.

Ans :

The domain names must be very unique and appropriate. The names should be selected from a names pace. The name space can be organized in two ways

(i) Flat name space

(ii) Hierarchical name space

(i) Flat name space

Flat name space is where the name is assigned to the IP address. They do not have any specific structure. In this flat name space, some meaningful names are given to IP address for accessing. The major disadvantage of flat name space is that they cannot be used in large system. Because they need to be accessed and controlled centrally to avoid ambiguity and redundancy. But it is difficult in flat name system. To avoid this major disadvantage hierarchical name space is used in large.

(ii) Hierarchical name space

Hierarchical name space is where the name is made up of several parts. The first part may represent the nature of organization, the second part may represent the name of organization, and third part may represent the department of the organization and so on. In this way the power to control the name space can be decentralized.

12. Resolutions in DNS.

Ans :

In DNS (Domain Name System), resolution refers to the process of translating a domain name into an IP address. When a user types a domain name into a web browser or other application, the DNS resolution process is initiated to translate the domain name into an IP address that can be used to locate the desired resource on the Internet.

13. SMI.

Ans :

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

14. SSL/TLS.

Ans :

SSL (Secure Sockets Layer) is a protocol used to provide secure communication over the internet. It is now commonly referred to as its successor protocol, TLS (Transport Layer Security), but the term SSL is still used colloquially to refer to this type of secure communication.

SSL works by encrypting the data exchanged between two parties, such as a web browser and a web server, to prevent it from being intercepted and read by unauthorized parties. The SSL protocol establishes a secure connection between the two parties, allowing them to exchange data in a secure and private manner.

15. PGP protocol.

Ans :

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.