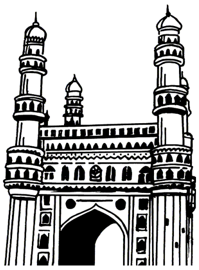
Rahul's ✔

Topper's Voice

NEW SYLLABUS



B.C.A.

I Year II Sem

Latest **2023** Edition

ADVANCED COMPUTER NETWORKS

☞ **Study Manual**

☞ **Important Questions**

☞ **Short Question & Answers**

☞ **Choose the correct Answers**

☞ **Fill in the blanks**

☞ **Solved Model Papers**

`.199/-

- by -

WELL EXPERIENCED LECTURER

Rahul Publications™

Hyderabad. Cell : 9391018098, 9505799122

All disputes are subjects to Hyderabad Jurisdiction only

B.C.A.

I Year II Sem

ADVANCED COMPUTER NETWORKS

Inspite of many efforts taken to present this book without errors, some errors might have crept in. Therefore we do not take any legal responsibility for such errors and omissions. However, if they are brought to our notice, they will be corrected in the next edition.

Price ` 199

Sole Distributors : **Cell : 9391018098, 9505799122**

VASU BOOK CENTRE

Shop No. 2, Beside Gokul Chat, Koti, Hyderabad.

Maternity Hospital Opp. Lane, Narayan Naik Complex, Koti, Hyderabad.
Near Andhra Bank, Subway, Sultan Bazar, Koti, Hyderabad -195.

CONTENTS

ADVANCED COMPUTER NETWORKS

STUDY MANUAL

SOLVED MODEL PAPERS

SYLLABUS

UNIT - I

NETWORK ARCHITECTURE, PERFORMANCE :

Bandwidth and Latency, High Speed Networks, Network-Centric View, Error Detection, Reliable Transmission, Ethernet and Multiple Access Networks, Overlay Networks: Routing Overlays, Peer-to-Peer Networks and Content Distribution Networks, Client-Server Networks, Delay-Tolerant Networks

UNIT - II

SWITCHING :

Circuit-Switched Networks, Datagram Networks, Virtual-Circuit Networks, Message Switched Networks, Asynchronous Transfer Mode: Evolution, Benefits, Concepts, Exploring Broadband Integrated Services Digital Network, Layer and Adaptation Layer

UNIT - III

IPv4 :

Address Space, Notations, Classful, Classless, Network Address Translation, Datagram, Fragmentation and Checksum IPv6 Addresses: Structure, Address Space, Packet Format and Extension Headers, ICMP, IGMP, ARP, RARP, Congestion Control and Resource Allocation: Problem, Issues, Queuing, TCP

UNIT - IV

CONGESTION CONTROL :

Congestion-Avoidance Mechanisms and Quality of Service, Internetworking: Intra-Domain and Inter-Domain Routings, Unicast Routing Protocols: RIP, OSPF and BGP, Multicast Routing Protocols: DVMRP, PIM-DM, PIM-SM, CBT, MSDP and MOSPF, Spanning Tree Algorithm

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.

Contents

Topic **Page No.**

UNIT - I

UNIT - II

UNIT - III

Topic **Page No.**

UNIT - IV

UNIT - V

Important Questions

UNIT - I

1. Write about different types of computer network architectures.

Ans :

Refer Unit-I, Q.No. 1.

2. What is Net-Centric Computing? Explain about its areas.

Ans :

Refer Unit-I, Q.No. 4.

3. What are different types of errors? Explain error detection techniques.

Ans ;

Refer Unit-I, Q.No. 5.

4. Write about various reliable services provided by transport layer.

Ans :

Refer Unit-I, Q.No. 6.

5. Write about peer to peer network.

Ans :

Refer Unit-I, Q.No. 12.

6. Explain about client server network.

Ans :

Refer Unit-I, Q.No. 16.

7. Explain about delay-tolerant network?

Ans:

Refer Unit-I, Q.No. 17.

UNIT - II

1. Explain about circuit switched networks.

Ans:

Refer Unit-II, Q.No. 1.

2. Explain about Datagram Networks.

Ans:

Refer Unit-II, Q.No. 3.

3. Write Differences between Virtual Circuits & Datagram Networks.

Ans:

Refer Unit-II, Q.No. 4.

4. What is Message Switching? Explain.

Ans:

Refer Unit-II, Q.No. 5.

5. What is Asynchronous Transfer Mode (ATM)? Expalin.

Ans:

Refer Unit-II, Q.No. 8.

6. Write about broadband integrated services.

Ans:

Refer Unit-II, Q.No. 10.

7. Explain about B-ISDN Architecture

Ans:

Refer Unit-II, Q.No. 11.

8. Explain B-ISDN layers for ATM.

Ans:

Refer Unit-II, Q.No. 12.

UNIT - III

1. What is address space? Explain about it.

Ans :

Refer Unit-III, Q.No. 1.

2. Explain about notations used in IPv4 and IPv6.

Ans :

Refer Unit-III, Q.No. 2.

3. What is Network Address Translation? Explain.

Ans :

Refer Unit-III, Q.No. 5.

4. Explain about datagram network.

Ans :

Refer Unit-III, Q.No. 11.

5. What is Fragmentation in Networking? Explain.

Ans :

Refer Unit-III, Q.No. 7.

6. What is Checksum? How to apply check-sum for error detection? Explain.

Ans :

Refer Unit-III, Q.No. 9.

7. Explain the structure of IPV6.

Ans :

Refer Unit-III, Q.No. 10.

8. Explain about IPv6 packet format and extension headers.

Ans :

Refer Unit-III, Q.No. 12.

UNIT - IV

1. What is congestion control? Explain the principles and techniques of congestion control.

Ans:

Refer Unit-IV, Q.No. 1.

2. Write the differences between Inter domain and Intradomain Routing.

Ans :

Refer Unit-IV, Q.No. 4.

3. Explain Distance Vector Multicast Routing Protocol.

Ans:

Refer Unit-IV, Q.No. 12.

4. Explain PIM-SM protocol.

Ans:

Refer Unit-IV, Q.No. 15.

5. What is MSDP protocol? Explain how to configure it.

Ans:

Refer Unit-IV, Q.No. 17.

6. Explain Spanning Tree algorithm working principle.

Ans:

Refer Unit-IV, Q.No. 19.

UNIT - V

1. What is SONET/SDH? Write SONET/SDH Transmission Standards.

Ans:

Refer Unit-V, Q.No. 1.

2. Explain the requirements of Traffic engineering.

Ans:

Refer Unit-V, Q.No. 2.

3. What is traffic sizing? Write about it

Ans:

Refer Unit-V, Q.No. 3.

4. Explain about the protocols used in traffic engieneering.

Ans:

Refer Unit-V, Q.No. 5.

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

Ans :

Refer Unit-V, Q.No. 7.

6. Write about the availability aspect in traffic engineering.

Ans:

Refer Unit-V, Q.No. 8.

7. Write about the availability aspect in traffic engineering.

Ans:

Refer Unit-V, Q.No. 9.

UNIT I

NETWORK ARCHITECTURE, PERFORMANCE :

Bandwidth and Latency, High Speed Networks, Network-Centric View, Error Detection, Reliable Transmission, Ethernet and Multiple Access Networks, Overlay Networks: Routing Overlays, Peer-to-Peer Networks and Content Distribution Networks, Client-Server Networks, Delay-Tolerant Networks

1.1 Network Architecture

Q1. Write about different types of computer network architectures.

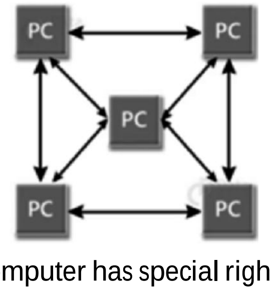
Ans : **(Imp.)**

Meaning

The design and setup of a computer network is called Computer Network Architecture. It is the organization and arrangement of different network devices (i.e., the clients such as PCs, desktops, laptops, mobiles etc.) at both physical and logical levels in order to fulfil the needs of the end user/ customer.

1. Peer-to-Peer Network

- The peers referred to here are the individual devices linked together directly, having equal responsibilities and equal powers without the presence of any central authority.
- Due to the absence of a central device in charge of tasks, this architecture is also known as decentralized architecture.



- Each computer has special rights for resource sharing, however this might cause issues if the computer with the resource is unavailable.
- Useful in smaller environments with less number of computers.

Advantages

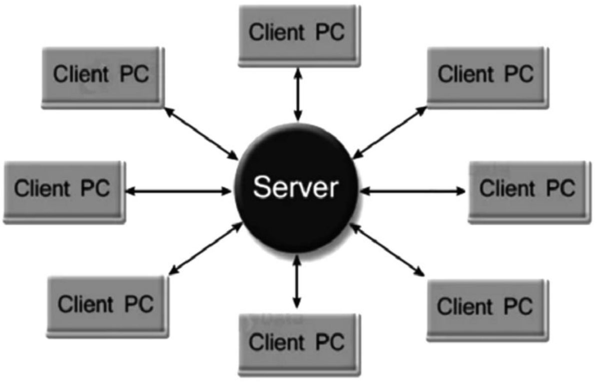
- No particular device is a client or a server, the tasks and responsibilities of servers are distributed among all the devices, which also act as clients.
- Very inexpensive to set up, as there is no requirement of a centralized server, and this also ensures that in case of any failure in the network, all unaffected devices continue to operate normally.
- It's simple to set up and maintain because each computer runs independently.

Disadvantages

- No centralized system, thus difficult to keep a backup of the data in case of any fault.
- It has a security flaw because the computers are self-managed.
- With a growth in the number of machines on this network, performance, security, and access may all become big issues.

2. Client-Server Architecture

- This is also known as centralized architecture, as one powerful central computer is in charge of serving all the requests from the client computers. This central computer is a server.
- The client computers connect to the server as and when they require the use of shared resources or shared data. All of the shared data is stored solely in the server, and not on any other computer.



- A server handles all of the key tasks, such as security and network administration.
- All of the clients interact with one another via a server.

Advantages

- This type of architecture is much easier to scale since it is much more convenient to add more server computers than configure the network on each and every computer (as is the case in peer-to-peer architecture).
- Much faster network speeds.
- Because a single server manages the shared resources in a Client/Server network, there is improvement in security.
- Backing up data is easy because of the centralized system.
- The server provides a customised Network Operating System (NOS) to offer resources to a large number of users that want them.

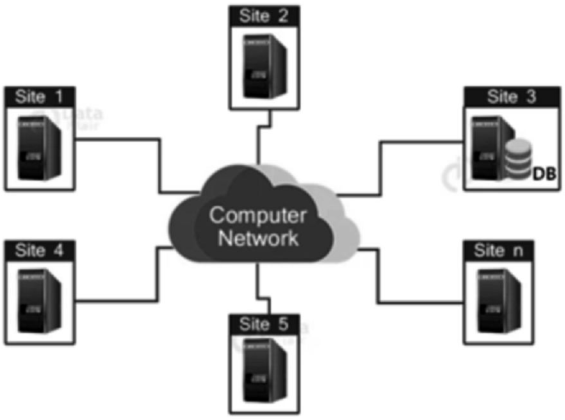
Disadvantages

- More prone to downtime because if the server fails, none of the client machines are able to get their requests served.
- Requirement of a dedicated network administrator to handle all of the resources.
- It is far more expensive than P2P. This is due to the requirement for a server with more RAM, as well as the necessity for several networking devices such as hubs, routers, switches, and so on.

There are some more lesser-known computer architectures:

3. Centralized Computing Architecture

One powerful computer is utilized to service one or more low-powered computers in centralized computing architecture. The nodes under the centralized architecture are not linked; they are only connected to the server.

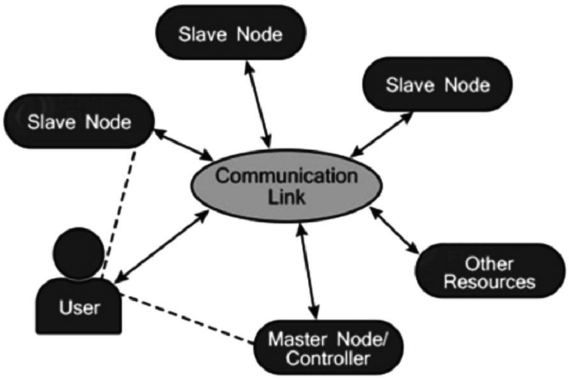


The centralized computing architecture includes the following components:

- The primary, mainframe computer which handles all processing.
- Terminals are connected to a central computer and function as input/output devices.
- Linking of at least two mainframe computers together via networks. Terminals communicate solely with the mainframe and never with one another.

4. Distributed Computing Architecture

A distributed architecture connects one or more nodes, which are personal computers. It supports a variety of functions, including file sharing, hardware sharing, and network sharing. The nodes in the distributed architecture can manage their own data and rely on the network for administration rather than data processing.

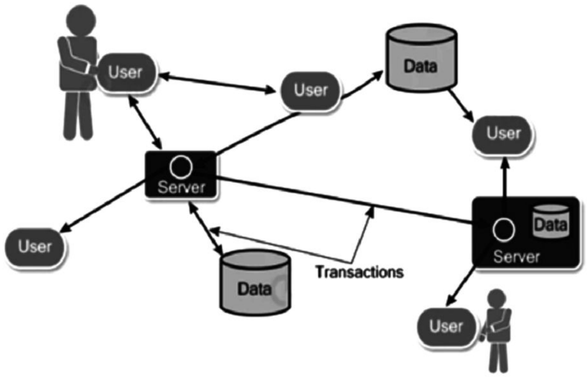


The following components are found in distributed computing architecture:

- Different computers are effective at performing independently.
- Completion of tasks on multiple computers locally.
- Networks enable computers to exchange data and services, but they do not offer processing help.

5. Collaborative Computing Architecture

The collaborative computing architecture is a hybrid of centralised and decentralised computing. Individual members of a network can process their users fundamental needs under the collaborative model.



A database server, such as an MSSQL server or an ORACLE server, for example, observes or manages all database-related operations on all network nodes. The model will, however, execute requests that are not from the database.

1.2 Performance

1.2.1 Bandwidth and Latency

Q2. Explain about bandwidth and Latency.

Ans :

Bandwidth

Bandwidth, or precisely network bandwidth, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time. That simply means that higher is the bandwidth of a network, larger is the amount of data network can be sending to and from across its path. Be careful not to confuse bandwidth with closely related terms such as the data rate and the throughput. Bandwidth is something that deals with the measurement of capacity and not the speed of data transfer.

Units of Measurement

Bandwidth is usually measured in bits transferred per second through a path or link. The common units of bandwidth we come across are as follows.

bps (Bits per second)

Mbps (Megabits per second)

Gbps (Gigabits per second)

Example :

Here, a bandwidth of 10 bps for a channel, is just another way of saying that a maximum of 10 bits can be transferred using that link for any given time. It has no relation with the transfer speed of the channel.

Latency

- Being simple latency means whenever you have given input to the system and the total time period it takes to give output so that particular time period/interval is known as latency.
- Actually, latency is the in-between handling time of computers, as some of you may think that whenever some system connects with another system it happens directly but no it isn't, the signal or data follows the proper traceroute for reaching its final destination.

- Nowadays fiber optic cables are used for transmitting the signals/data from one place to another with the speed of light but obviously before reaching to the final destiny the data/signal has to pass from many checkpoints or posts and follow a proper traceroute so it takes some time to get respond from the receiver and that total round of time is known as latency.
- If you want to know the fastest possible network connection you could have from one place to another then we will suppose light as a medium because light just takes 100milli seconds(approx.) to take a round of earth. So according to the data if you let light as a medium then you can send 20 packets per second across the other sides of the world.

1.2.2 High Speed Networks

Q3. Explain about High Speed Networks.

Ans :

1. Switched Ethernet

Switched Ethernet relies on centralized multiport switches to provide a physical link between multiple LAN segments. Inside each intelligent switch, high-speed circuitry supports wire-speed virtual connections between all the segments for maximum bandwidth allocation on demand. Adding new segments to a switch increases the aggregate network speed while reducing overall congestion, so Switched Ethernet provides superior configuration flexibility. It also gives you an excellent migration path from 10- to 100-Mbps Ethernet because both segments can often operate via the same switch.

Benefits

It's a cost-effective technique for increasing the overall network throughput and reducing congestion on a 10-Mbps network. Other than the addition of the switching hub, the Ethernet network remains the same the same network interface cards, the same client software, the same LAN cabling.

100BASE-T (IEEE 802.3u)

100BASE-T retains the familiar CSMA/CD media access technique used in 10-Mbps Ethernet networks. It also supports a broad range of cabling options: two standards for twisted pair, one for fiber. 100BASE-TX supports 2-pair Category 5 UTP or Type 1 STP cable. 100BASE-T4 uses 4-pair Category 3 or 4 cable. And 100BASE-FX supports fiber optic links via duplex multimode fiber cable.

Benefits

It retains CSMA/CD, so existing network management systems don't need to be rewritten. It can easily be integrated into existing 10-Mbps Ethernet LANs, so your previous investment is saved. It's also backed by hundreds of manufacturers in the high-speed networking industry.

100VG (IEEE 802.12)

100VG uses an encoding scheme called Quartet Signaling to transmit data simultaneously over all four pairs in the network cable, so it achieves a full tenfold increase in transmission speeds over 10BASE-T. It also replaces the CSMA/CD media access control protocol with Demand Priority to optimize network operation and eliminate the overhead of packet collisions and recovery. Demand Priority works like this: The hub directs all transmissions, acknowledging higher-priority packet requests before normal-priority requests. This effectively guarantees bandwidth to time-sensitive applications like voice, video, and multimedia applications.

Benefits

It uses a transmission frequency very similar to traditional Ethernet, works on any conventional cabling system (Category 3, 4, or 5 UTP, Type 1 STP, and fiber optics), and uses the same connectors. In addition, 100VG may soon support Token Ring networks a potential advantage over its rival standard 100BASE-T.

2. ATM

Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication technique that supports data-transfer rates ranging from sub-T1 speeds (less than 1.544 Mbps) up to 10 Gbps. Like other packet-switching services (Frame Relay, SMDS), ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. Instead, it relies on the inherent integrity of digital lines to ensure data integrity.

Benefits

Networks are extremely versatile. An ATM network can be treated as a single network, whether it connects points in a building or across the country. Its fixed-length cell-relay operation, the signaling technology of the future, offers more predictable performance than variable-length frames. And it can be integrated into an existing network as needed without having to upgrade the entire LAN.

3. FDDI

FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the token ring protocol.

In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network(WAN).

An FDDI network contains two token rings, one for possible backup in case the essential ring falls flat.

The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps

Characteristics

- FDDI gives 100 Mbps of information throughput.
- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

Advantages of FDDI

- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

Disadvantages

- FDDI is complex. Thus establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically since fiber optic cable, connectors and concentrators are exceptionally costly.

4. Frame Relay

Frame Relay (frame relay) is a packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection.

It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends. It makes it more efficient than X.25, and a higher process speed achieved (it can transmit over 2,044 Mbps).

If the traffic is hefty, with a large number of small packages, its performance is more excellent than X25.

If large files transferred at high speeds, the price/performance ratio is higher in X25.

Frame relay has evolved from X.25 packet switching and objective is to reduce network delays, protocol overheads and equipment cost. Error correction is done on an end-to-end basis rather than a link -to-link basis as in X.25 switching. Frame relay can support multiple users over the same line and can establish a permanent virtual circuit or a switched virtual circuit.

Frame relay is considered to be a protocol, which must be carried over a physical link. While useful for connection of LANs, the combination of low throughput, delay variation and frame discard when the link is congested will limit its usefulness to multimedia.

- Packet switching was developed when the long distance digital communication showed a large error rate.
- To reduce the error rate, additional coding bits were introduced in each packet in order to introduce redundancy to detect and recover errors.
- But in the modem high speed telecommunication a system, this overhead is unnecessary and infect counter productive.
- Frame relay was developed for taking the advantage of the high data rates and low error rates in the modem communication system.
- The original packet switching networks were designed with a data rate at the user end of about 64 kbps.
- But the frame relay networks are designed to operate efficiently at the user's data rates upto 2 Mbps.
- This is possible practically because most of the overhead (additional bits) are striped off.
- Frame relay is a virtual circuit wide area network which was designed in early 1990s.
- Frame relay also is meant for more efficient transmission scheme than the X.25 protocol.
- Frame Relay is used mostly to route Local Area Network protocols such as IPX or TCP/IP.

Characteristics

1. Frame Relay service is a service that supports the transport of data
2. Frame relay is a connectionless service, meaning that each data packet passing through the network contains -address information
3. Frame relay is a service that is provided with a variety of speeds from 56 Kbs up to 25 Mbs.
4. Even though the most used speeds for the service are currently 56 Kbs and 1.544 Mbs
5. Frames are variable in length and goes up to 4,096 bytes
6. Frame Relay is considered to be a Broadband ISDN service
7. One of the unique facets of frame relay service is that the service supports variable size data packets.

Features

Some important features of frame relay are :

1. Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).
2. Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
3. It allows the bursty data.
4. It has a large frame size of 9000 bytes. So it can accommodate all local area network frame sizes.
5. Frame relay can only detect errors (at the data link layer). But there is no flow control or error control.
6. The damaged frame is simply dropped. There is no retransmission. This is to increase the speed. So frame relay needs a reliable medium and protocols having flow and error control.

5. SONET

The synchronous optical network or SONET is a standardized form of protocol that is used in digital communication between the sender and the receiver. SONET protocol uses fiber optic medium (optical fibers) to transmit a huge amount of data across a large distance. One of the main advantages that a synchronous optical network provides is that it can be used to transfer multiple streams of data simultaneously (at the same time) using optical fibers.

Some of the important points related to SONET are:

- SONET is used in the physical layer of the OSI model for broadband synchronized transmission of data such as voice, video, etc.
- It was developed by Bellcore in the mid-1980s and it was developed for the public telephone network.
- It is used in the North American region.
- SONET is standardized by the American National Standards Institute (ANSI).
- SONET is efficient and costs low for a few channels because of higher transmission rates.
- SONET is somewhat similar to the SDH which is used in the regions like Japan and Europe.
- At the higher capabilities, there is a problem with bandwidth efficiency.
- There is more overhead related to the SONET protocol as it is complex to implement and we have to work with multiple channels.
- There is no standard compatible with the SONET protocol.
- Tributary services are used for transporting and switching payloads and for the tributary services, the mux services of SONET are necessary.

Advantages

- Transmits data to large distances
- Low electromagnetic interference
- High data rates
- Large Bandwidth

Disadvantages

- No standard that is compatible.
- SONET mux services are necessary for tributary services.
- Low cost and efficient for few channels.
- The SONET/SDH network management system is inadequate for managing and using the DWDM technique.
- At higher capacities, bandwidth efficiency is a problem.
- There must be more overhead.

1.2.3 Network-Centric View

Q4. What is Net-Centric Computing? Explain about its areas.

Ans : **(Imp.)**

Meaning

Net-Centric Computing (NCC) is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network. Net-centric Computing focuses on large-scale distributed computing systems and applications that communicate through open, wide-area networks like the Internet. General examples of large-scale network-centric systems are the World-Wide Web and Computational Grids.

Net-centric computing refers to an emerging technology architecture and an evolutionary stage of client/server computing. It is a common architecture built on open standards that supports in different ways for different people to collaborate and to reach different information sources.

The evolutionary nature of net-centric computing links technological capabilities and strategic opportunities, helping people in facing today’s new problems and providing the flexibility to meet tomorrow’s challenges.

Areas

There is a wide array of subject areas, the most important of which are;

1. Web Applications

A web application (or web app) is an application software that runs on a web server. Web applications are accessed by the user through a web browser with an active network connection. Some examples of commonly-used web applications can be stated as web-mail, online retail sales, online banking, and online auctions. Web applications can be designed for a wide variety of users and can be used by anyone for numerous reasons.

Functionality

For proper functioning a web application requires three elements; a web server to handle requests from the client, an application server to execute the tasks requested by the user and a database to store information. Typical web application flow can be described in five steps;

1. User presents a request to the web server over the Internet, through a web browser or the application's user interface.
2. Web server sends this request to the appropriate web application server.
3. Web application server performs the requested task and then generates the results of the requested data.
4. Web application server sends results to the web server with the requested information or processed data.
5. Web server responds to the client with the requested information that then appears on the user's display.

Development

Development of a web application has two phases as front-end and back-end development. Front-end development is the client-side development and scripting languages like JavaScript, HTML5, or Cascading Style Sheets (CSS) are commonly used for the process.

Design

Web application design is an important stage in building a web application. It focuses on the appearance and feel of the web application to the user. This stage encompasses several different aspects, including user interface design (UI), usability design(UX), content production, and graphic design. UI stands for User Interface. UI is the part of the web application with which a user interacts. Simply, it's everything you see and touch, such as buttons, colors, fonts, navigation, etc. UX stands for User Experience. UX focuses on users' experience and feeling towards their journey through the web app. Was the web application hard to use, was it slow, was the user disappointed when using it? are the criteria mainly considered by a UX designer.

Security

Attacks against web apps range from database manipulation to large-scale network disruption. Some of the common methods of attack are;

- Cross site scripting (XSS)
- SQL injection (SQi)
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Buffer overflow
- Cross-site request forgery (CSRF)
- Data breach

General yet some of important steps in ensuring security and gaining the customer trust, can be stated as using up-to-date encryption, requiring proper authentication, continuously patching discovered vulnerabilities, and having good software development hygiene.

2. Distributed Systems

Introduction

A distributed system is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another from any system in order to appear as a single system to the end-user. The computers that are in a distributed system can be physically together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible components, such as mainframes, personal computers, workstations, minicomputers, and so on. Common use cases of a distributed systems are electronic banking systems, massive multiplayer online games, and sensor networks.

Functionality

There are two general ways that distributed systems function :

1. Each component of the system works to achieve a common goal and the end-user views results as one combined unit.
2. Each component has its own end-user and the distributed system facilitates sharing resources or communication services.

Architectural models

Distributed systems generally consist of four different basic architectural models :

1. **Client-server :** Clients contact the server for data, then format it and display it to the end-user.
2. **Three-tier :** Information about the client is stored in a middle tier rather than on the client, to simplify application deployment.
3. **n-tier :** Generally used when the server needs to forward requests to additional enterprise services on the network.
4. **Peer-to-peer :** There are no additional nodes used to provide services or manage resources. Responsibilities are uniformly distributed among components in the system, known as peers, which can serve as either client or server.

3. Cloud Computing

Cloud computing is the delivery of different computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet without direct active management by the user. Simply stating, cloud computing means storing and accessing data and programs over the internet instead of ones' computer's hard drive. Organizations are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics, and customer-facing web applications. As an example, healthcare services use the cloud to develop more personalized treatments for patients. Financial services are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to players around the world.

Security

Cloud security is a discipline of cyber security committed to secure cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms. Cloud security is a key concern for cloud storage providers. Major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, insecure application program interfaces (APIs) and Distributed denial of service (DDoS) attacks. Some common methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections.

4. Semantic Web

"The Semantic Web is a webby way to link data" — Dave Beckett

Introduction

The Semantic Web is an extension of the existing World Wide Web, extended with the goal of the making network data machine-understandable. In other words, the current Web is transformed from being machine-readable to machine understandable. The Semantic Web provides much smarter and more effortless customer experiences by giving content in the forms compatible to a customer's need. It not only improves traditional search, but is facilitating more seamless, intelligent, and integrated customer experience journeys as well. Semantic Web represents the next vital evolution in connecting information.

1.2.4 Error Detection

Q5. What are different types of errors? Explain error detection techniques.

Ans ; **(Imp.)**

Errors in Communication

When the information received at the receiver end does not match the sent data. At the time of transmission, errors are introduced into the binary data sent from the sender to the receiver due to noise during transmission. This means that a bit having a 0 value can change to 1 and a bit having a 1 value can change to 0.

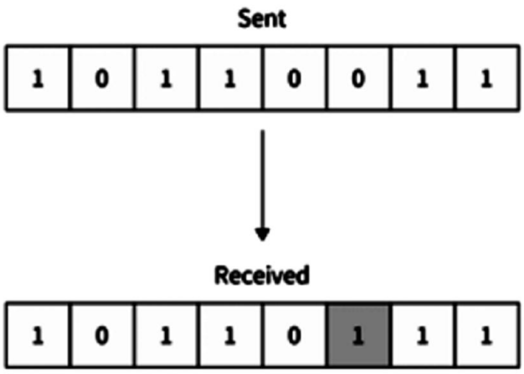
Types of Errors

Some errors that occur during communication are given below:

1. Single-bit Error

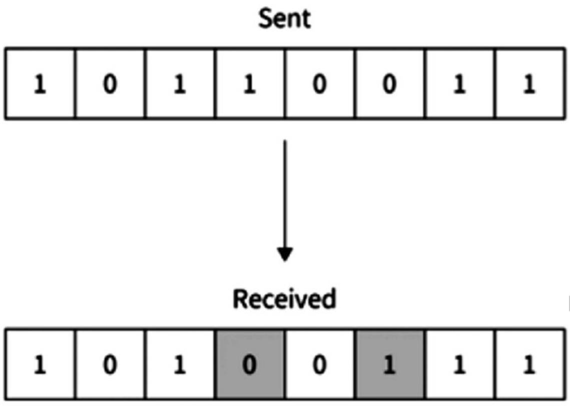
Typically, only one bit of the frame received is corrupt, and the corrupted bit can be located anywhere in the frame.

Refer to the below image for the single-bit error



2. Multiple-bit Error

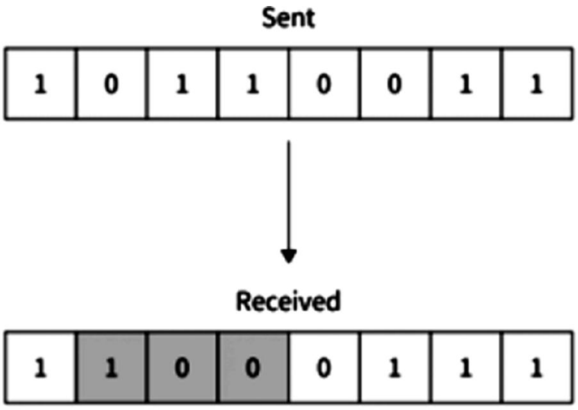
More than one bit received in the frame is found to be corrupted. Refer to the below image for the multiple-bit error



3. Burst Error

More than one consecutive bit is corrupted in the received frame.

Refer to the below image for the burst-bit error



Error Detection techniques

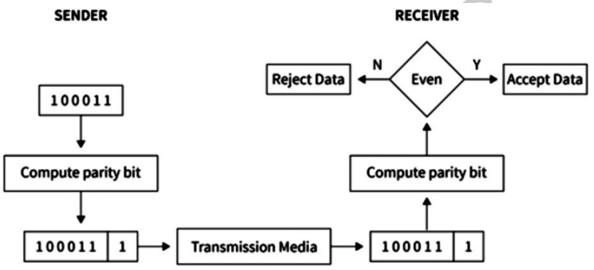
1. Simple Parity Check

Data sent from the sender undergoes parity check :

- 1 is added as a parity bit to the data block if the data block has an odd number of 1's.
- 0 is added as a parity bit to the data block if the data block has an even number of 1's.

This procedure is used for making the number of 1's even. And this is commonly known as even parity checking.

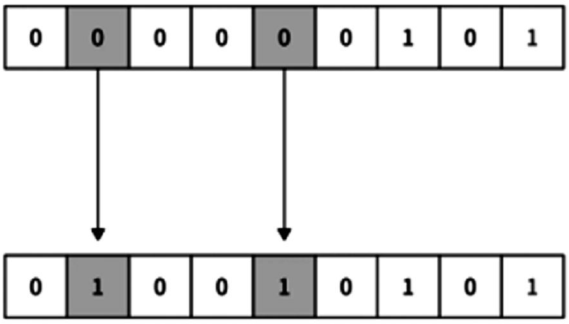
Refer to the below image for the simple parity-checking method :



Disadvantage

- Only single-bit error is detected by this method, it fails in multi-bit error detection .
- It can not detect an error in case of an error in two bits.

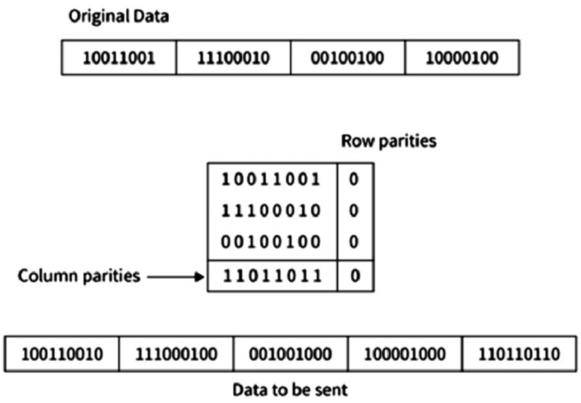
Refer to the below image for the disadvantage simple parity checking method



2. Two-Dimensional Parity Check

For every row and column, parity check bits are calculated by a simple method of parity check. Parity for both rows and columns is transmitted with the data sent from sender to receiver. At the receiver's side, parity bits are compared with the calculated parity of the data received.

Refer to the below image for the two-dimensional parity checking method



Disadvantages

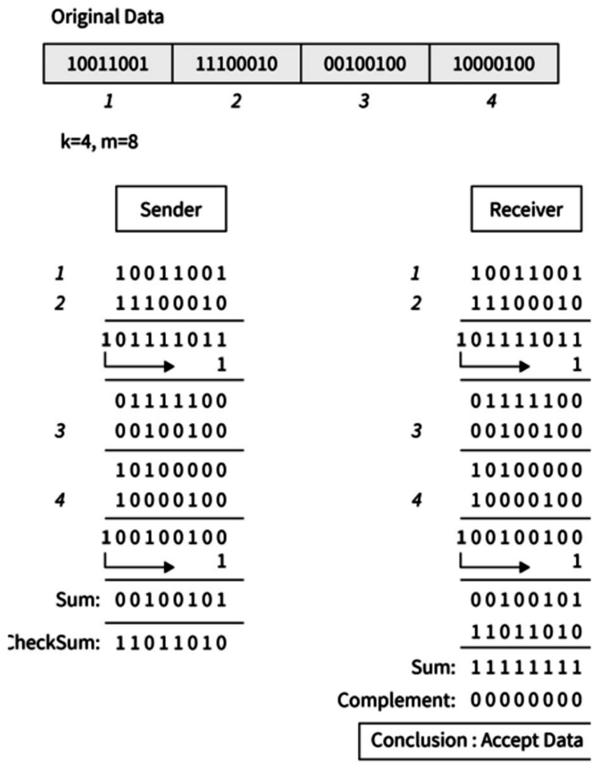
- ➢ If 2 bits are corrupted in 1 data unit and another data unit exactly at the same position is corrupted then this method is not able to detect the error.
- ➢ Sometimes this method is not used for **detecting 4-bit **errors or more than 4-bit errors.

3. Checksum

Checksum is a error detection which detects the error by dividing the data into the segments of equal size and then use 1's complement to find the sum of the segments and then sum is transmitted with the data to the receiver and same process is done by the receiver and at the receiver side, all zeros in the sum indicates the correctness of the data.

1. First of all data is divided into k segments in a checksum error detection scheme and each segment has m bits.
2. For finding out the sum at the sender's side, all segments are added through 1's complement arithmetic. And for determining the checksum we complement the sum.
3. Along with data segments, the checksum segments are also transferred.
4. All the segments that are received on the receiver's side are added through 1S complement arithmetic to determine the sum. Then complement the sum also.
5. The received data is accepted only on the condition that the result is found to be 0. And if the result is not 0 then it will be discarded.

Refer to the below image for the checksum method

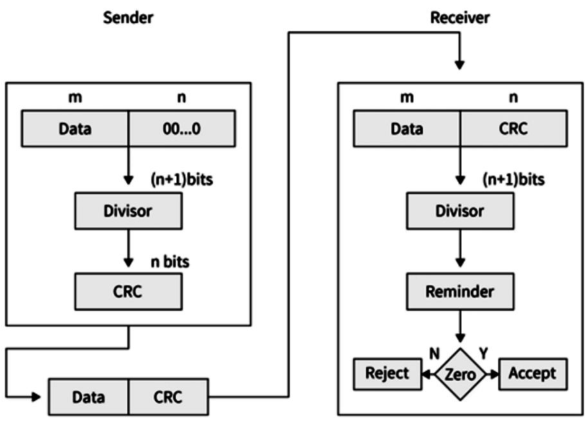


Disadvantages

In checksum error is not detected, if one sub-unit of the data has one or more corrupted bits and corresponding bits of the opposite value are also corrupted in another sub-unit. Error is not detected in this situation because in this case the sum of columns is not affected by corrupted bits.

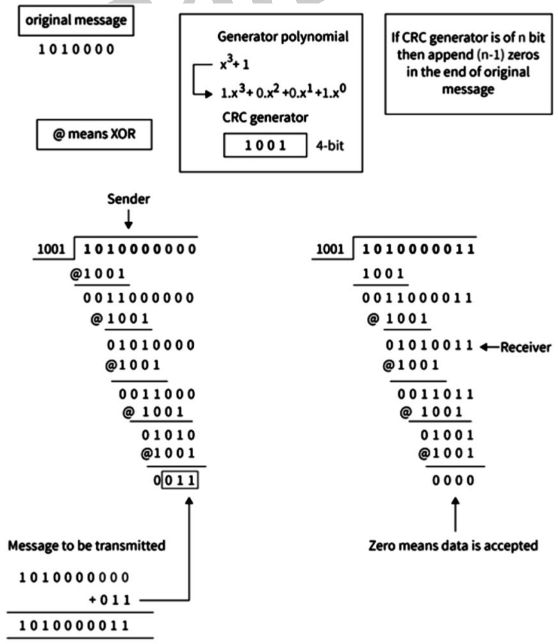
4. Cyclic Redundancy Check

Refer to the below image for the cyclic redundancy checking method



- The checksum scheme uses the addition method but CRC uses binary division.
- A bit sequence commonly known as cyclic redundancy check is added to the end of the bits in CRC. This is done so that the resulting data unit will be divisible by the second binary number that is predetermined.
- The receiving data units on the receiver's side need to be divided by the same number. These data units are accepted and found to be correct only on the condition of the remainder of this division is zero. The remainder shows that the data is not correct. So, they need to be discarded.

Refer to the below image for the example of the cyclic redundancy checking method



Disadvantages

Cyclic Redundancy Check may leads to overflow of data.

1.2.5 Reliable Transmission

Q6. Write about various reliable services provided by transport layer.

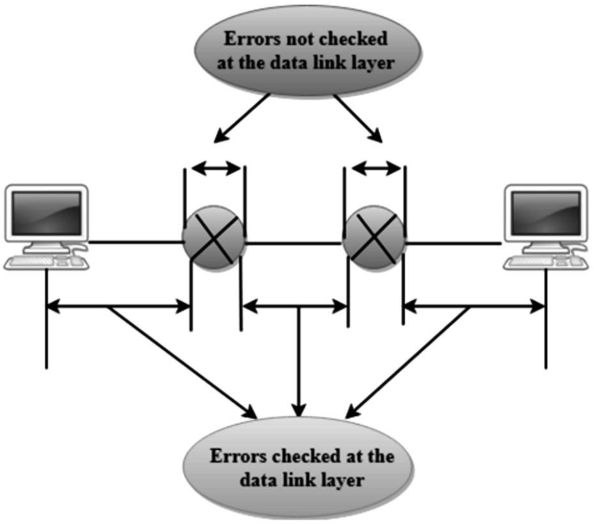
Ans : **(Imp.)**

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects :

1. Error Control

- The primary role of reliability is Error Control. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.


Errors not checked at the data link layer
Errors checked at the data link layer

- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

2. Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

3. Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

4. Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

5. Flow Control

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Q7. What is multiplexing? Write about stop and wait protocol.

Ans :

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.

Stop and Wait protocol

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

The primitives of stop and wait protocol are:

Sender side

Rule 1:

Sender sends one data packet at a time.

Rule 2:

Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

Receiver side

Rule 1:

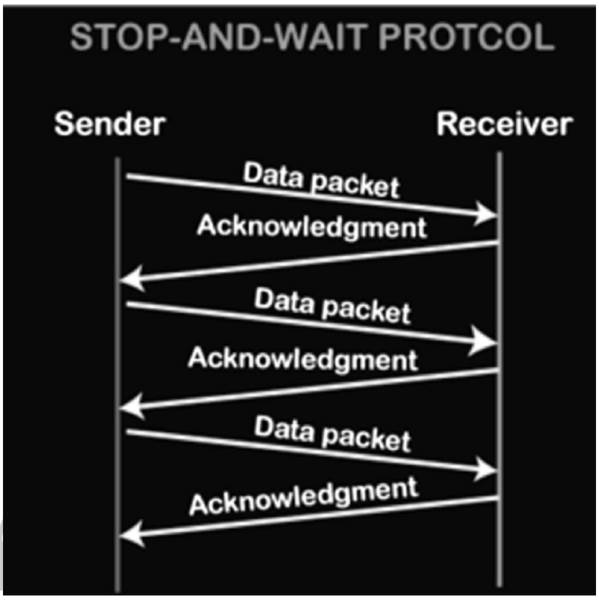
Receive and then consume the data packet.

Rule 2:

When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.

Working of Stop and Wait protocol

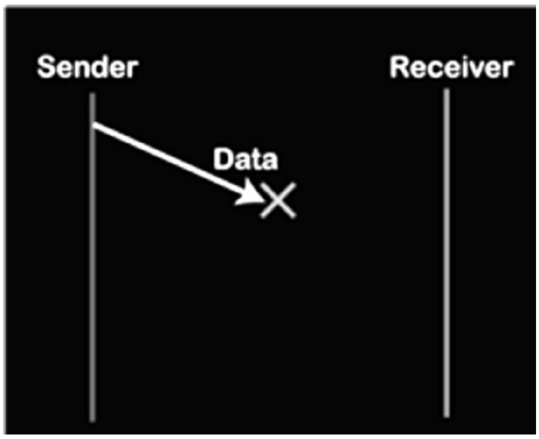


The above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Disadvantages

The following are the problems associated with a stop and wait protocol:

1. Problems occur due to lost data

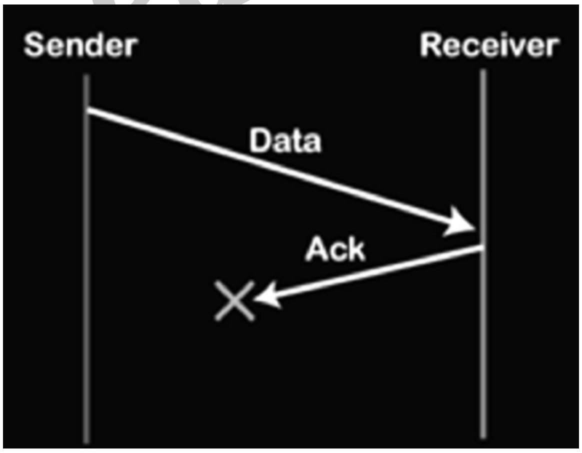


Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

- Sender waits for an infinite amount of time for an acknowledgment.
- Receiver waits for an infinite amount of time for a data.

2. Problems occur due to lost acknowledgment

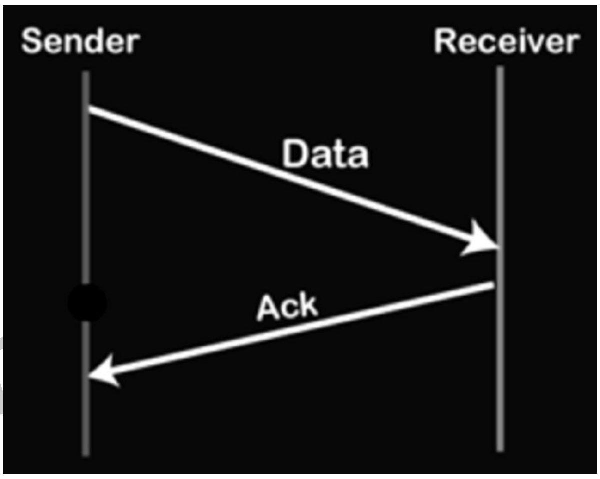


Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

In this case, one problem occurs

- Sender waits for an infinite amount of time for an acknowledgment.

3. Problem due to the delayed data or acknowledgment



Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.

Q8. Explain Sliding window protocol.

Ans :

A sliding window is also known as windowing. A sliding window is a method for controlling sending data packets between two network devices where dependable and sequential delivery of data packets is needed, such as using the Data Link Layer (OSI model) or Transmission Control Protocol (TCP).

In the sliding window technique, each data packet (for most data link layers) and byte (in TCP) includes a unique consecutive sequence number used by the receiving computer to place data in the correct order. The objective of the sliding window technique is to use the sequence numbers to avoid duplicate data and to request missing data.

Following are the two types of Sliding Window Protocol :

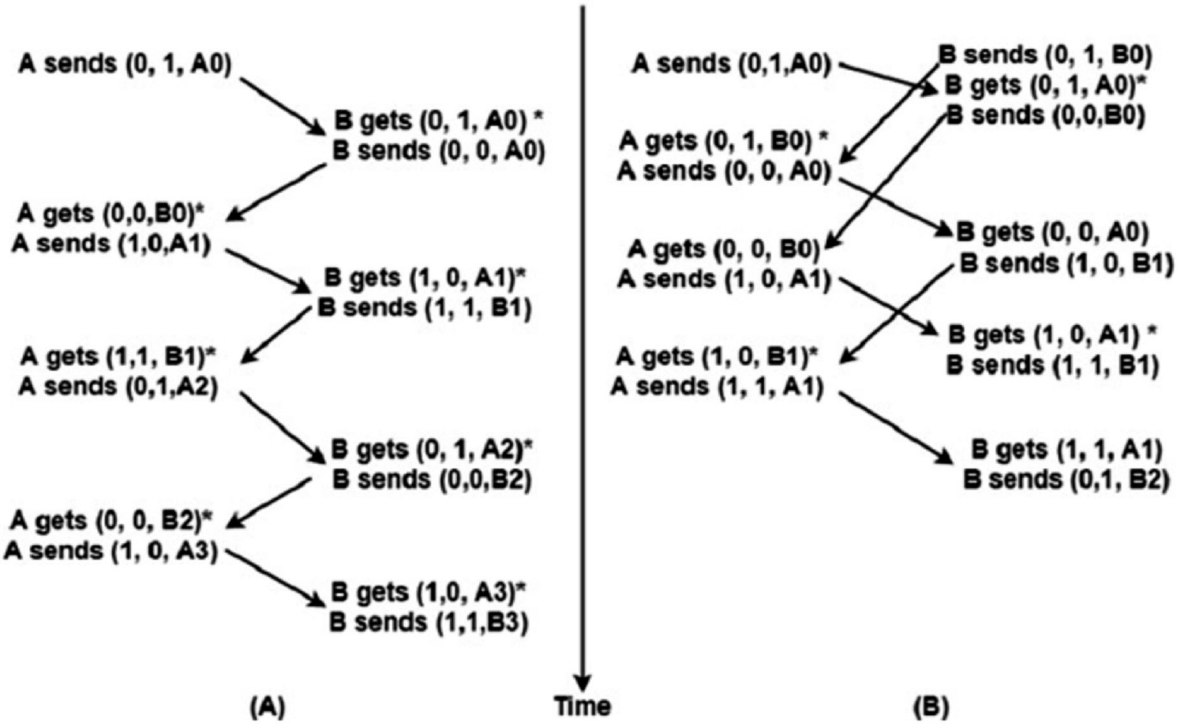
Go Back-n Protocol

Go-Back-N Automatic Repeat Query (ARQ) protocol is also referred to as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that helps a sliding window method. In this, if any frame is manipulated or lost, all subsequent frames have to be sent again.

For example, in GO- Back –N, the N is the sender's window size; if it is GO-Back-5, the sender will send frame 1 to 5 before receiving the knowledge of frame 1.

All the frames are numbers to deal with the most and duplicate frames. If the sender does not receive the receiver's acknowledgement, then all the frames available in the current window will be re-transmitted.

The design of the Go-Back-N protocol is shown below :



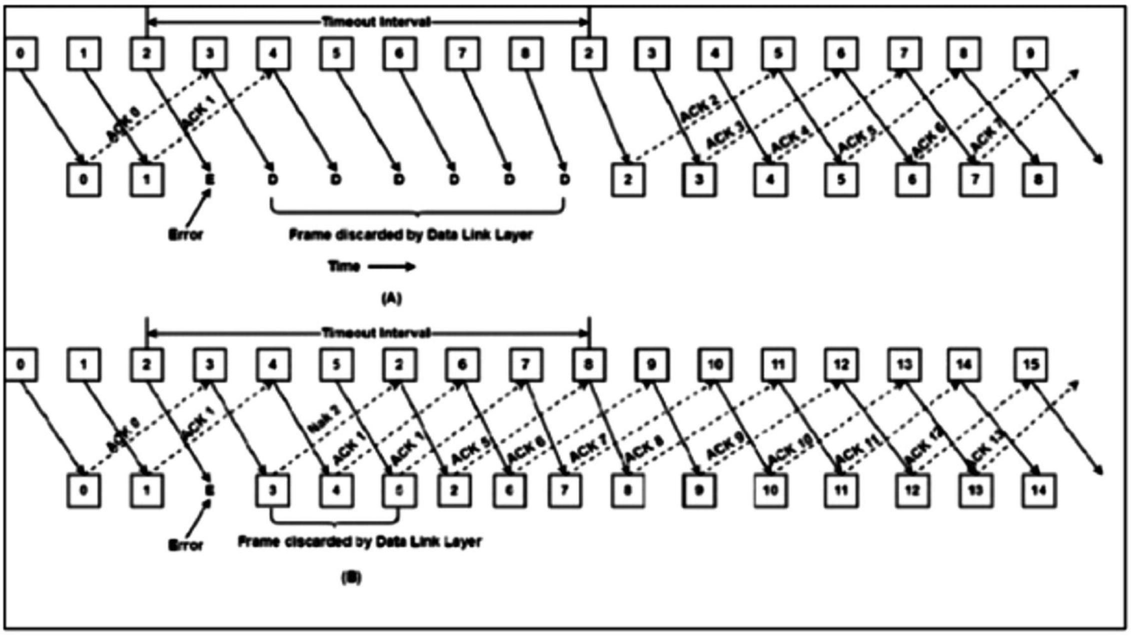
Selective Repetitive ARQ

Selective Repeat ARQ is also referred to as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that facilitates a sliding window method. The Goback-N ARQ protocol operates well if it has fewer errors.

In this protocol, the sender window size is always similar to the size of the receiver window. The size of the sliding window is continually greater than 1.

If the receiver obtains a corrupt frame, it does not directly remove it. It sends a negative acknowledgement to the sender. The sender sends that frame again immediately, receiving a negative acknowledgement. There is no waiting for any time-out to share that frame.

The structure of the Selective Repeat ARQ protocol is demonstrated below :



1.2.6 Ethernet And Multiple Access Networks

Q9. Explain about multi access networks.

Ans :

The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD).

As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link.

The Ethernet has its roots in an early packet radio network, called Aloha, developed at the University of Hawaii to support computer communication across the Hawaiian Islands. Like the Aloha network, the fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently (in Aloha, the medium was the atmosphere, while in the Ethernet the medium was originally a coax cable). The core idea in both Aloha and the Ethernet is an algorithm that controls when each node can transmit.

Physical Properties

Ethernet segments were originally implemented using coaxial cable of length up to 500 m. (Modern Ethernets use twisted copper pairs, usually a particular type known as “Category 5,” or optical fibers, and in some cases can be quite a lot longer than 500 m.) This cable was similar to the type used for cable TV. Hosts connected to an Ethernet segment by tapping into it. A *transceiver*, a small device directly attached to the tap, detected when the line was idle and drove the signal when the host was transmitting. It also received incoming signals. The transceiver, in turn, connected to an Ethernet adaptor, which was plugged into the host. This configuration is shown in Figure.

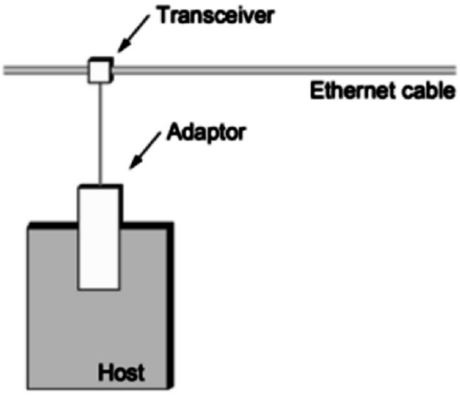


Fig.: Ethernet transceiver and adaptor

Multiple Ethernet segments can be joined together by repeaters (or a multi-port variant of a repeater, called a hub). A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals; repeaters do not understand bits or frames. No more than four repeaters could be positioned between any pair of hosts, meaning that a classical Ethernet had a total reach of only 2500 m. For example, using just two repeaters between any pair of hosts supports a configuration similar to the one illustrated in Figure, that is, a segment running down the spine of a building with a segment on each floor.

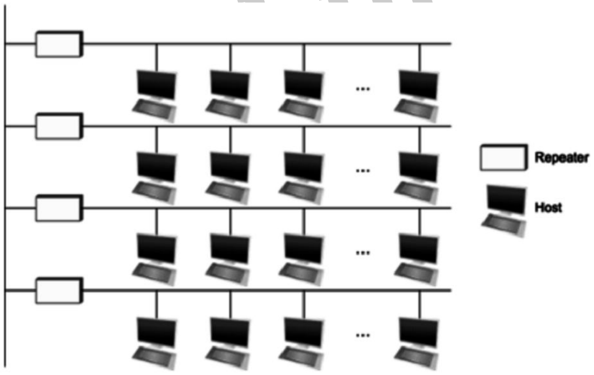


Fig.: Ethernet repeater, interconnecting segments to form a larger collision domain.

Any signal placed on the Ethernet by a host is broadcast over the entire network; that is, the signal is propagated in both directions, and repeaters and hubs forward the signal on all outgoing segments. Terminators attached to the end of each segment absorb the signal and keep it from bouncing back and interfering with trailing signals. The original Ethernet specifications used the Manchester encoding scheme described in an earlier section, while 4B/5B encoding (or the similar 8B/10B) scheme is used today on higher speed Ethernets.

It is important to understand that whether a given Ethernet spans a single segment, a linear sequence of segments connected by repeaters, or multiple segments connected in a star configuration, data transmitted by any one host on that Ethernet reaches all the other hosts.. The multi-access part of the Ethernet is all about dealing with the competition for the link that arises in a collision domain.

Access Protocol

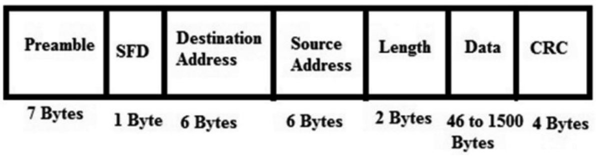
We now turn our attention to the algorithm that controls access to a shared Ethernet link. This algorithm is commonly called the Ethernet's media access control (MAC). It is typically implemented in hardware on the network adaptor. We will not describe the hardware per se, but instead focus on the algorithm it implements. First, however, we describe the Ethernet's frame format and addresses.

Ethernet Protocol Frame Structure

Generally, the structure of the Ethernet frame is defined within the IEEE 802.3 standard. But there are numerous optional frame formats are being employed for Ethernet to expand the capacity of the protocol. The Early frame versions were very slow but the latest Ethernet versions operate at 10 Gigabits/sec. So this is the very fastest Ethernet version.

The frame structure at the data link layer in the OSI model is almost the same for all Ethernet speeds. The structure of the frame simply adds headers & trailers in the region of the Layer 3 PDU (Protocol Data Unit) to summarize the message. The frame structure of Ethernet is shown below and it begins with the Preamble that functions at the physical layer

Ethernet header includes both Source & Destination MAC address, after which the frame's payload is present. The end field is Cyclical Redundancy Checking, used to notice the error. The following diagram shows the structure of the frame & fields.



Ethernet Frame Structure

Preamble

The first pattern of the Ethernet Protocol frame is 7-Bytes of Preamble where alternative 0's and 1's in this frame indicate the beginning of the frame & permit the sender & receiver to set up bit-level synchronization. At first, a Preamble in the above frame was introduced to permit for the few bits loss because of signal delays.

However, present high-speed-based Ethernet doesn't require Preamble for protecting the frame bits. Preamble specifies the receiver that frame is coming & lets the receiver lock on the data stream before the genuine frame starts.

Start of Frame Delimiter

The start of frame delimiter (SFD) is a 1-Byte field with 10101011 values that indicates that upcoming bits are the beginning of the frame, which is the address of the destination. The start of the frame delimiter is mainly designed to split the pattern of the bit to the preamble & signal the beginning of the frame.

Sometimes, the start of frame delimiter is considered as the main part of the preamble, so this is the main reason that Preamble is expressed as 8 Bytes in several places. The SFD gives a warning to stations that this is the final opportunity for synchronization.

Destination Address

The Destination Address Field is a 6-bytes field in the above Ethernet frame. The address within the frame & the device MAC address is compared. If both the addresses are matched, then the device simply allows the frame. This MAC address is a unicast, multi-cast, or broadcast.

Source Address

The source address is a 6-Byte field, including the source machine's MAC address. Once the address of source is an individual address or Unicast always, then LSB of an initial byte will be always.

Length

This field size is 2-byte long that specifies the entire Ethernet frame length. The length value held by the 16-bit field ranges from 0 to 65534, however, the length cannot be higher than 1500 due to some own Ethernet limitations.

Data Field

Data field is the location where actual data can be added and it is also called Payload. Here, both the data & IP header will be inserted if IP is used over Ethernet. So, the highest data available may be 1500 Bytes. If the data length is below the minimum length of 46 bytes, then padding zeros can be included to reach the minimum achievable length.

CRC Field

The CRC in the frame is the last pattern with 4 Bytes. This field includes 32-bits of data hash code, which is produced over the Source Address, Destination Address, Length, and Ethernet Protocol's Data field. If the checksum is calculated through a destination that is not similar to the sent checksum value, then received data can be corrupted.

Here, the frame size for IEEE 802.3 Ethernet standard changes from 64 bytes – 1518 bytes with 46 to 1500 bytes of data length.

Addresses

Each host on an Ethernet—in fact, every Ethernet host in the world—has a unique Ethernet address. Technically, the address belongs to the adaptor, not the host; it is usually burned into ROM. Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons. Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped. For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address

000010000000000000101011111001001011000100000010

To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build. For example, Advanced Micro Devices has been assigned the 24-bit prefix 080020 (or 8:0:20). A given manufacturer then makes sure the address suffixes it produces are unique.

Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet. Each adaptor recognizes those frames addressed to its address and passes only those frames on to the host. (An adaptor can also be programmed to run in *promiscuous* mode, in which case it delivers all received frames to the host, but this is not the normal mode.) In addition to these *unicast* addresses, an Ethernet address consisting of all 1s is treated as a *broadcast* address; all adaptors pass frames addressed to the broadcast address up to the host. Similarly, an address that has the first bit set to 1 but is not the broadcast address is called a multicast address. A given host can program its adaptor to accept some set of multicast addresses. Multicast addresses are used to send messages to some subset of the hosts on an Ethernet (e.g., all file servers). To summarize, an Ethernet adaptor receives all frames and accepts

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode

It passes to the host only the frames that it accepts

1.3 Overlay Networks

1.3.1 Routing Overlays

Q10. Write about overlay networks.

Ans :

An overlay network is a virtual or logical network that is created on top of an existing physical network. The internet, which connects many nodes via circuit switching, is an example of an overlay network.

An overlay network is any virtual layer on top of physical network infrastructure. This may be as simple as a virtual local area network (VLAN) but typically refers to more complex virtual layers from software-defined networking (SDN) or a software-defined wide area network (SD-WAN).

The overlay creates a new layer where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links. Overlays enable administrators to define and manage traffic flows, irrespective of the underlying physical infrastructure.

Overlay networks and SDN

SDN is a quickly growing network strategy where the network operating system separates the data plane (packet handling) from the control plane (the network topology and routing rules). SDN acts as an overlay, running on the distributed switches, determining how packets are handled, instead of a centralized router handling those tasks.

SDN enables more flexible virtual networking that enables a more hands-off approach without changes to the physical underlay. SDN is an example of distributed computing where the actual processing is spread across multiple nodes, a departure from client-server computing where those routes were hardcoded.

Overlay network structure and protocols

Overlay network protocols include Virtual Extensible LAN (VXLAN), Generic Routing Encapsulation, Network Virtualization using GRE, Stateless Transport Tunneling and Network Virtualization Overlays.

Most network overlays work at Layer 3 in the Open Systems Interconnection (OSI) model, handling all traffic through the IP address. But, if a VLAN is created as an overlay, then the overlay would be done at Layer 2 with media access control (MAC) addresses.

In the case of SDN, the most common protocol for communication is OpenFlow, an open standard protocol that provides interoperability and is used in some fashion by most SDN tools.

Advantages

Network overlays provide some key benefits to networking, including the following:

- **Flexibility :** The overlay provides a more flexible networking approach by removing the hardcoded constraints of a physical network, which enables configuration tied to usage or function.

- **Management :** Overlays offer better access management by segmenting and joining devices logically instead of managing these components physically.
- **Security :** Overlay networks enhance security by segmenting traffic and restricting access by groups, individuals or devices. In the case of a network compromise — when using SDN as an overlay — an attacker's traffic can be detected and stopped more easily.
- **Redundancy and efficiency :** With an overlay, traffic has an easier time changing routes based on either traffic saturation or network interruptions.

Disadvantages

Despite the advantages of overlay networks, organizations should heed the potential challenges or disadvantages as well, including the following:

- **Extra layers of management :** IT would have to manage two different network layers daily. Most importantly, the layers must be managed in unison as the topology that the overlay expects needs to be accurately represented in the underlay.
- **Troubleshooting :** Again, this must occur for both the underlay and overlay.
- **Potential security exposure.** The negative effects of misconfiguration can be amplified across a wider set of devices or users.

Examples and uses of overlay networks

Some examples of overlay network deployments include virtual private networks, peer-to-peer networks, content delivery networks, voice over IP services and non-native software-defined networks. Other examples and uses of overlay networks are the following:

- **VLAN or VXLAN :** These networks are created at Layer 2 or encapsulated with Layer 2 to create logical segments for routing traffic.
- **Hypervisor and virtual servers :** Virtual networking creates virtual switches and virtual network cards that create an overlay for communicating between virtual machines or between the hypervisor and the rest of the network.
- **SD-WAN :** SD-WAN creates an overlay that manages a communication tunnel between two networks so that all the communications do not need to be hardcoded to the connection.
- **SDN :** SDN uses protocols like OpenFlow to create a virtual overlay that sits on top of network switches, enabling the switches to handle more of the data routing functions, optimizing data flow.

Q11. Explain about routing overlays.

Ans :

The simplest kind of overlay is one that exists purely to support an alternative routing strategy; no additional application-level processing is performed at the overlay nodes. You can view a virtual private network (VPN) as an example of a routing overlay, but one that doesn't so much define an alternative strategy or algorithm as it does alternative routing table entries to be processed by the standard IP forwarding algorithm.

As hosts they are probably connected to the Internet by only one physical link, but as a node in the overlay they would be connected to multiple neighbours via tunnels.

Since overlays, almost by definition, are a way to introduce new technologies independent of the standardization process, there are no standard overlays we can point to as examples..

Experimental Versions of IP

Overlays are ideal for deploying experimental versions of IP that you hope will eventually take over the world. For example, IP multicast started off as an extension to IP and even today is not enabled in many Internet routers. The MBone (multicast backbone) was an overlay network that implemented IP multicast on top of the unicast routing provided by the Internet. A number of multimedia conference tools were developed for and deployed on the Mbone.

Like VPNs, the MBone used both IP tunnels and IP addresses, but unlike VPNs, the MBone implemented a different forwarding algorithm—forwarding packets to all downstream neighbors in the shortest path multicast tree. As an overlay, multicast-aware routers tunnel through legacy routers, with the hope that one day there will be no more legacy routers.

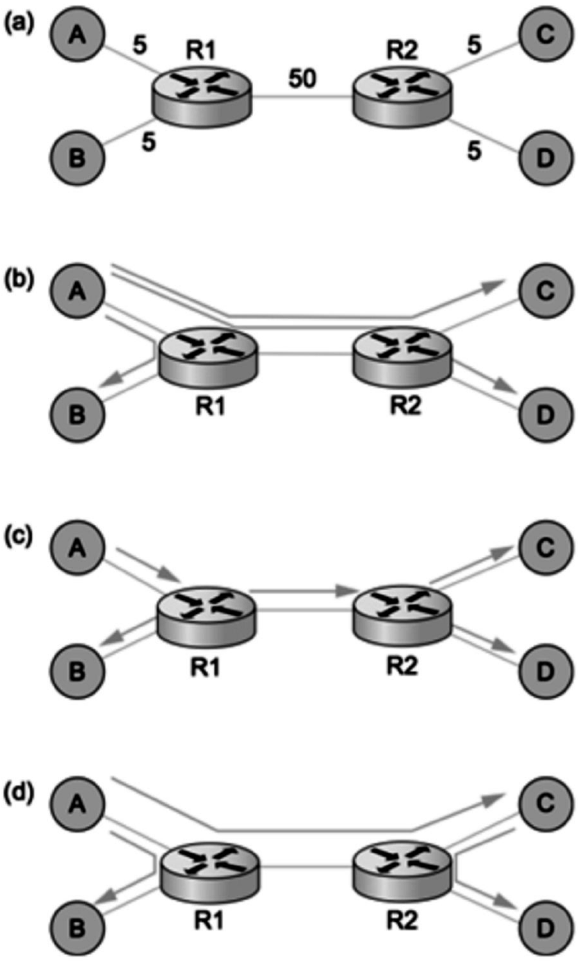
The 6-BONE was a similar overlay that was used to incrementally deploy IPv6. Like the MBone, the 6-BONE used tunnels to forward packets through IPv4 routers. Unlike the MBone, however, 6-BONE nodes did not simply provide a new interpretation of IPv4's 32-bit addresses. Instead, they forwarded packets based on IPv6's 128-bit address space. The 6-BONE also supported IPv6 multicast.

End System Multicast

Although IP multicast is popular with researchers and certain segments of the networking community, its deployment in the global Internet has been limited at best. In response, multicast-based applications like video conferencing have recently turned to an alternative strategy, called end system multicast. The idea of end system multicast is to accept that IP multicast will never become ubiquitous and to instead let the end hosts that are participating in a particular multicast-based application implement their own multicast trees.

Before describing how end system multicast works, multicast assumes that only Internet hosts (as opposed to Internet routers) participate in the overlay. Moreover, these hosts typically exchange messages with each other through UDP tunnels rather than IP tunnels, making it easy to implement as regular application programs.

This makes it possible to view the underlying network as a fully connected graph, since every host in the Internet is able to send a message to every other host. Abstractly, then, end system multicast solves the following problem: Starting with a fully connected graph representing the Internet, the goal is to find the embedded multicast tree that spans all the group members.



Since we take the underlying Internet to be fully connected, a naive solution would be to have each source directly connected to each member of the group. In other words, end system multicast could be implemented by having each node send unicast messages to every group member. To see the problem in doing this, especially compared to implementing IP multicast in routers, consider the example topology in Figure.

Figure, depicts an example physical topology, where R1 and R2 are routers connected by a low-bandwidth transcontinental link; A, B, C, and D are end hosts; and link delays are given as edge weights. Assuming A wants to send a multicast message to the other three hosts, Figure 1 shows how naive unicast transmission would work. This is clearly undesirable because the same message must traverse the link A-R1 three times, and two copies of the message traverse R1-R2.

Figure, depicts the IP multicast tree constructed by the Distance Vector Multicast Routing Protocol (DVMRP). Clearly, this approach eliminates the redundant messages. Without support from the routers, however, the best one can hope for with end system multicast is a tree similar to the one shown in Figure 1. End system multicast defines an architecture for constructing this tree.

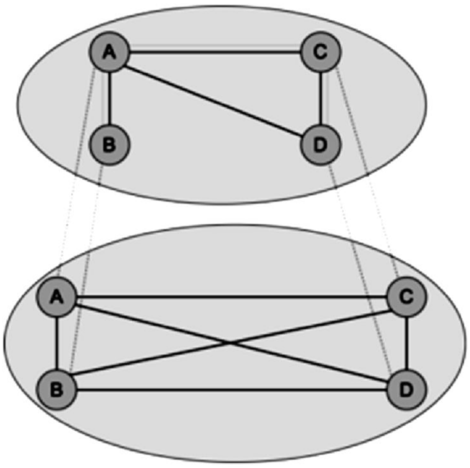


Fig.: Multicast tree embedded in an overlay network

The general approach is to support multiple levels of overlay networks, each of which extracts a subgraph from the overlay below it, until we have selected the subgraph that the application expects. For end system multicast, in particular, this happens in two stages: First we construct a simple mesh overlay on top of the fully connected Internet, and then we select a multicast tree within this mesh.

The idea is illustrated in Figure 2, again assuming the four end hosts A, B, C, and D. The first step is the critical one: Once we have selected a suitable mesh overlay, we simply run a standard multicast routing algorithm (e.g., DVMRP) on top of it to build the multicast tree.

The key to constructing the intermediate mesh overlay is to select a topology that roughly corresponds to the physical topology of the underlying Internet, but we have to do this without anyone telling us what the underlying Internet actually looks like since we are running only on end hosts and not routers. The general strategy is for the end hosts to measure the roundtrip latency to other nodes and decide to add links to the mesh only when they like what they see. This works as follows.

First, assuming a mesh already exists, each node exchanges the list of all other nodes it believes is part of the mesh with its directly connected neighbours. When a node receives such a membership list from a neighbour, it incorporates that information into its membership list and forwards the resulting list to its neighbours. This information eventually propagates through the mesh, much as in a distance vector routing protocol.

When a host wants to join the multicast overlay, it must know the IP address of at least one other node already in the overlay. It then sends a “join mesh” message to this node. This connects the new node to the mesh by an edge to the known node. In general, the new node might send a join message to multiple current nodes, thereby joining the mesh by multiple links. Once a node is connected to the mesh by a set of links, it periodically sends “keepalive” messages to its neighbours, letting them know that it still wants to be part of the group.

When a node leaves the group, it sends a “leave mesh” message to its directly connected neighbours, and this information is propagated to the other nodes in the mesh via the membership list described above. Alternatively, a node can fail or just silently decide to quit the group, in which case its neighbours detect that it is no longer sending “keep alive” messages. Some node departures have little effect on the mesh, but should a node detect that the mesh has become partitioned due to a departing node, it creates a new edge to a node in the other partition by sending it a “join mesh” message.

As described so far, we will end up with a mesh that is a subgraph of the original fully connected Internet, but it may have suboptimal performance because

1. Initial neighbour selection adds random links to the topology.
2. Partition repair might add edges that are essential at the moment but not useful in the long run.
3. Group membership may change due to dynamic joins and departures.
4. Underlying network conditions may change.

What needs to happen is that the system must evaluate the value of each edge, resulting in new edges being added to the mesh and existing edges being removed over time.

To add new edges, each node i periodically probes some random member j that it is not currently connected to in the mesh, measures the round-trip latency of edge (i, j), and then evaluates the utility of adding this edge. If the utility is above a certain threshold, link (i, j) is added to the mesh. Evaluating the utility of adding edge (i, j) might look something like this:

1.3.2 Peer-to-Peer Networks and Content Distribution Networks

Q12. Write about peer to peer network.

Ans :

A peer-to-peer network is a simple network of computers. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

History

Before the development of P2P, USENET came into existence in 1979. The network enabled the users to read and post messages. Unlike the forums we use today, it did not have a central server. It is used to copy the new messages to all the servers of the node.

- In the 1980s the first use of P2P networks occurred after personal computers were introduced.
- In August 1988, the internet relay chat was the first P2P network built to share text and chat.
- In June 1999, Napster was developed which was a file-sharing P2P software. It could be used to share audio files as well. This software was shut down due to the illegal sharing of files. But the concept of network sharing i.e P2P became popular.
- In June 2000, Gnutella was the first decentralized P2P file sharing network. This allowed users to access files on other users' computers via a designated folder.

Types

1. **Unstructured P2P networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content. For example, Napster, Gnutella, etc.
2. **Structured P2P networks:** It is designed using software that creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set up but can give easy access to users to the content. For example, P-Grid, Kademlia, etc.
3. **Hybrid P2P networks:** It combines the features of both P2P networks and client-server architecture. An example of such a network is to find a node using the central server.

Features

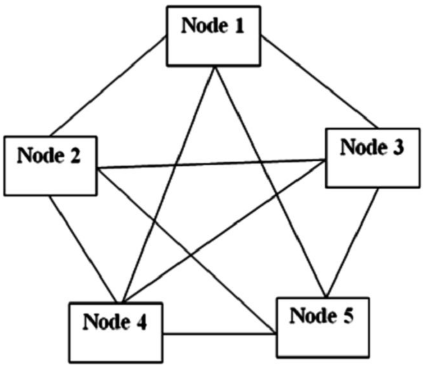
- These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.
- Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network.
- Since the nodes act as clients and servers, there is a constant threat of attack.
- Almost all OS today support P2P networks.

P2P Network Architecture

In the P2P network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printers.

- Each computer in the network has the same set of responsibilities and capabilities.
- Each device in the network serves as both a client and server.

- The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.
- Each computer in the network has the ability to share data with other computers in the network.
- The architecture is usually composed of workgroups of 12 or more computers.



How Does P2P Network Work?

Let's understand the working of the Peer-to-Peer network through an example. Suppose, the user wants to download a file through the peer-to-peer network then the download will be handled in this way:

- If the peer-to-peer software is not already installed, then the user first has to install the peer-to-peer software on his computer.
- This creates a virtual network of peer-to-peer application users.
- The user then downloads the file, which is received in bits that come from multiple computers in the network that have already that file.
- The data is also sent from the user's computer to other computers in the network that ask for the data that exist on the user's computer.

Thus, it can be said that in the peer-to-peer network the file transfer load is distributed among the peer computers.

How to Use a P2P Network Efficiently?

Firstly secure your network via privacy solutions. Below are some of the measures to keep the P2P network secure:

- **Share and download legal files:** Double-check the files that are being downloaded before sharing them with other employees. It is very important to make sure that only legal files are downloaded.
- **Design strategy for sharing:** Design a strategy that suits the underlying architecture in order to manage applications and underlying data.
- **Keep security practices up-to-date:** Keep a check on the cyber security threats which might prevail in the network. Invest in good quality software that can sustain attacks and prevent the network from being exploited. Update your software regularly.
- **Scan all downloads:** This is used to constantly check and scan all the files for viruses before downloading them. This helps to ensure that safe files are being downloaded and in case, any file with potential threat is detected then report to the IT Staff.
- **Proper shutdown of P2P networking after use:** It is very important to correctly shut down the software to avoid unnecessary access to third persons to the files in the network. Even if the windows are closed after file sharing but the software is still active then the unauthorized user can still gain access to the network which can be a major security breach in the network.

Q13. State the applications of P2P Network.

Ans :

Below are some of the common uses of P2P network:

- **File sharing:** P2P network is the most convenient, cost-efficient method for file sharing for businesses. Using this type of network there is no need for intermediate servers to transfer the file.
- **Blockchain:** The P2P architecture is based on the concept of decentralization. When a peer-to-peer network is enabled on the blockchain it helps in the maintenance of a complete replica of the records ensuring the

accuracy of the data at the same time. At the same time, peer-to-peer networks ensure security also.

- **Direct messaging:** P2P network provides a secure, quick, and efficient way to communicate. This is possible due to the use of encryption at both the peers and access to easy messaging tools.
- **Collaboration:** The easy file sharing also helps to build collaboration among other peers in the network.
- **File sharing networks:** Many P2P file sharing networks like G2, and eDonkey have popularized peer-to-peer technologies.
- **Content distribution:** In a P2P network, unline the client-server system so the clients can both provide and use resources. Thus, the content serving capacity of the P2P networks can actually increase as more users begin to access the content.
- **IP Telephony:** Skype is one good example of a P2P application in VoIP.

Q14. Explain the advantages and disadvantages of P2P Network.

Ans :

Advantages of P2P Network

- **Easy to maintain:** The network is easy to maintain because each node is independent of the other.
- **Less costly:** Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
- **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
- **Adding nodes is easy:** Adding, deleting, and repairing nodes in this network is easy.
- **Less network traffic:** In a P2P network, there is less network traffic than in a client/ server network.

Disadvantages of P2P Network

- **Data is vulnerable:** Because of no central server, data is always vulnerable to getting lost because of no backup.
- **Less secure:** It becomes difficult to secure the complete network because each node is independent.
- **Slow performance:** In a P2P network, each computer is accessed by other computers in the network which slows down the performance of the user.
- **Files hard to locate:** In a P2P network, the files are not centrally stored, rather they are stored on individual computers which makes it difficult to locate the files.

Examples of P2P networks

P2P networks can be basically categorized into three levels.

- The first level is the basic level which uses a USB to create a P2P network between two systems.
- The second is the intermediate level which involves the usage of copper wires in order to connect more than two systems.
- The third is the advanced level which uses software to establish protocols in order to manage numerous devices across the internet.

Some of the popular P2P networks are Gnutella, BitTorrent, eDonkey, Kazaa, Napster, and Skype.

Q15. What is a Content Distribution Network and how does it work?

Ans :

A CDN is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content. A CDN-

1. Manages servers that are geographically distributed over different locations.
2. Stores the web content in its servers.
3. Attempts to direct each user to a server that is part of the CDN so as to deliver content quickly.

How does CDN work?

To minimize the distance between the visitors and your website's server, a CDN stores a cached version of original content in multiple geographical locations (a.k.a., points of presence/ PoPs). Each PoP contains a number of caching servers known as edge servers that are responsible for content delivery to visitors within its proximity. CDN caches content in many places at once, ensuring quick delivery of content.

Let's consider an example:

Suppose you are hosting a website, wherein your origin server(server containing the primary source of your website's data, where website files are hosted) is located in Australia and a company XYZ provides you the CDN service.

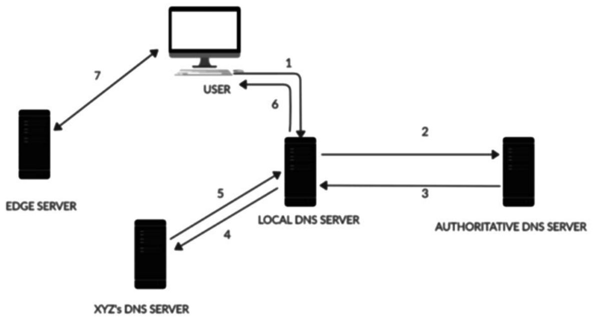
When a user in India clicks on a video on your website, the request goes to the user's local DNS server(See DNS), which relays the request to the authoritative DNS server of your website.

The authoritative DNS server then identifies that the user is situated far away and therefore relays the request to its XYZ's DNS server. Now the DNS query enters XYZ's network which provides the address of the edge server that is closest to the user to the Local DNS server. The video is delivered by this edge server.

From this point onwards the local DNS server knows the address of the edge server. So whenever users within its network send a request for content from your website, the local DNS server shall relay the request to the edge server.

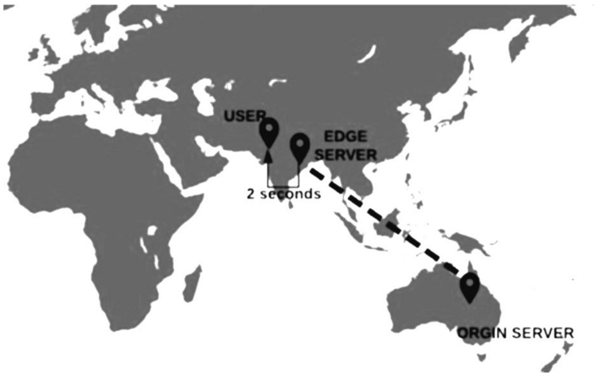
CDN thus minimizes the number of hops required to deliver the data to a user's browser due to the POPs that are located near the user.

Following image depicts the same:

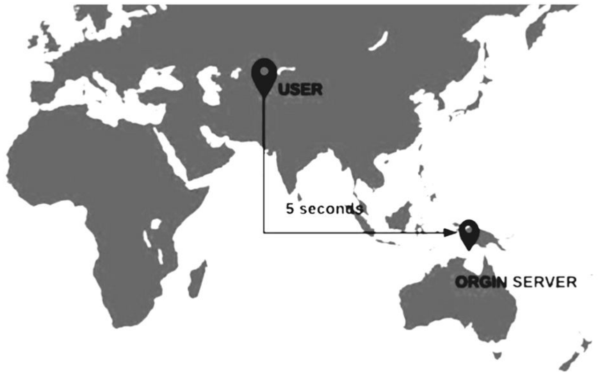


Following Image depicts the difference between how a request is handled with and without a CDN respectively:

WITH CDN(2 SECONDS)



WITHOUT CDN(5 SECONDS)



1.3.3 Client-Server Network

Q16. Explain about client server network.

Ans :

In client-server network relationships, certain computers act as servers and others act as clients.

A server is simply a computer that provides the network resources and provides service to other computers when they request it. A client is the computer running a program that requests the service from a server. Local area network (LAN) is based on client server network relationship.

A client-server network is one on which all available network resources such as files, directories, applications and shared devices, are centrally managed and hosted and then are accessed by the client.

Client server networks are defined by the presence of servers on a network that provide security and administration of the network.

How Does a Client-Server Network Work?

Before jumping to the main topic of learning how a client-server network works, let's first learn about the hardware used in a client-server network.

Clients' hardware is typically a PC or other mobile device that comes preloaded with network apps. The person on the other side of the computer sends a request to the server via the internet.

As you may have guessed by now, the one that resides on the server-side is a 'server' or data centre that stores myriads of data in files, databases, and applications.

Now we know the hardware used in a client-server network, so let's look at the working of the client-server network:

The client-server network works based on the principle of a two-way street, where the client sends the requests simultaneously and sends an update and appropriate results for the requested queries.

A client-server network comprises multiple clients and servers; therefore, network traffic can be significant. To save bandwidth on the network, the server shuts the connection to the client once the job is completed. As a result, the speed with which results are delivered is determined by the bandwidth efficiency of the client and server.

The client-server architecture can be utilised both on the internet and in a local area network (LAN), such as in a company or organisation.

Advantages

The client-server architectural concept has several advantages:

- **Centralization:** A single server that houses all of the essential data in one location makes data security and user authorization and authentication control much easier. Any issue that arises throughout the whole network may be resolved in a single location.
- **Scalability:** A client-server network may be expanded by adding network segments, servers, and PCs with little downtime. Client-server networks offer scalability. The number of resources, such as clients and servers, can be increased as needed by the user. Consequently, the server's size may be increased without any disruptions. Since the server is centralized, there are no questions regarding access to network resources even as the size grows. As a result, just a small number of staff members are needed for the setups.
- **Easy Management:** Clients and the server do not have to be close to access data effectively. It is really simple to handle files because they are all kept on the same server. The finest management for tracking and finding records of necessary files is offered in client-server networks.
- **Accessibility:** The client-server system's nodes are all self-contained, requesting data only from the server, allowing for simple upgrades, replacements, and relocation.
- **Data Security:** The centralized design of a client-server network ensures that the data is properly safeguarded. Access controls can be used to enforce it and ensure that only authorized users are allowed access. Imposing credentials like a username and password is one such technique. Additionally, if the data were to be destroyed, it would be simple to restore the files from a single backup.

Disadvantages

The client-server network has a few disadvantages:

- **Network Traffic Congestion:** The main disadvantage of a client-server model is the danger of a system overload owing to a lack of resources to service all of the clients. If too many different clients try to connect to the shared network at the same time, the connection may fail or slow down. Additionally, if the internet connection is down, any website or client in the world will be unable to access the information. Large businesses may be at risk if they are unable to get important information.
- **High Cost:** In client-server networks, the cost of setting up and maintaining the server is typically higher than the cost of running the network. The networks might be expensive to buy because of their strength. The users won't all be able to afford them as a result.

- **Robustness:** The whole network will be interrupted, if the primary server experiences failure or interference. Client-server networks lack hence in terms of resilience, since client-server networks are centralized.
- **Maintenance Difficulty:** When the servers are put in place, they will run continuously, which implies they need to receive the necessary care. If there are any mistakes, they must be fixed right away without further delay. As a result, a qualified network manager should be hired to look after the server.
- **Unacquirable Resources:** Not all of the resources on the server are available for acquisition. For instance, you cannot immediately print a document from the web or change any information stored on the client's hard drive.

Types of Clients

Clients are computer hardware or server software that makes requests for resources and services that a server makes available. Clients are often referred to as "service requesters". Thick, Thin, or Hybrid client computing are the three categories.

- **Thick Client:** A client that offers extensive functionality, does the majority of data processing on its own, and depends on the server only a little.
- **Thin Client:** An application server handles the majority of the necessary data processing for a thin-client server, which is a lightweight computer that heavily relies on the resources of the host computer.
- **Hybrid Client:** A hybrid client combines the elements of a thin client and a thick client. It may do local processing but must rely on the server to keep persistent data.

Types of Servers

The different types of servers are given below :

- **File server :** These servers provide the services for storing, retrieving and moving the data. A user can read, write, exchange and manage the files with the help of file servers.
- **Printer server :** The printer server is used for controlling and managing printing on the network. It also offers the fax service to the network users.
- **Application server :** The expensive software and additional computing power can be shared by the computers in a network with the help of application servers.
- **Message server :** It is used to co-ordinate the interaction between users, documents and applications. The data can be used in the form of audio, video, binary, text or graphics.
- **Database server :** It is a type of application server.

1.3.4 Delay-Tolerant Networks

Q17. Explain about delay-tolerant network?

Ans : **(Imp.)**

A delay-tolerant network (DTN) is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

In such environments, the conventional internet does not work; networks are also subject to frequent disruptions, high error rates and latency of hours or even days. A DTN can overcome such challenges and reliably transmit information, ensuring dependable internet working.

Need

Introduced in 2003, delay-tolerant networks have proved most useful in deep space communications. In space, communications between Earth and spacecrafts involve long distances of thousands and even millions of miles, consequently making delays, disruptions, errors and data losses inevitable. Existing terrestrial networking technologies proved unable to handle such issues, which must be addressed at the application level. That's where DTNs come in.

The Consultative Committee for Space Data Systems (CCSDS) has developed other protocols that incorporate some aspects of delay-tolerant networking. However, they cannot provide the same level of flexibility or automated data transfer as DTNs.

Two such protocols are Space Packet Protocol and CCSDS File Delivery Protocol:

- **Space Packet Protocol:** This protocol can forward packets across a managed data path through the network. However, it cannot address the scheduled nature of connectivity, which may be why it has not been implemented in a space system.
- **CCSDS File Delivery Protocol (CFDP):** CFDP provides reliable delivery of files, but it is limited to file transfers only. It does not support messaging, streaming or other applications.

Advantages of delay-tolerant networks

DTN is a suite of protocols developed by the Delay & Disruption Tolerant Networking Research Group administered by the Internet Engineering Task Force (IETF). These protocols are versatile enough to operate either with terrestrial IP protocols or independently

Terrestrial IP networks are based on store-and-forward operation. However, they assume that the storing will persist for only a modest amount of time, depending on the queuing and transmission delay.

DTN architecture expects nodes to store bundles for an extended period. Whenever possible, each received data packet is forwarded immediately. If forwarding is not currently possible but is expected to be possible in the future, the packet is stored for future transmission. Thus, when using a DTN, only the next hop is required to be available. Delay-tolerant networking uses this automatic store-and-forward mechanism to assure data delivery, which conventional terrestrial networks cannot do.

Other important benefits of DTNs include the following :

- enabled interoperability of ground stations and spacecraft;
- more efficient data transmissions and more usable bandwidth;
- improved link reliability;
- support for integrity checks, authentication and encryption for more secure communications; and
- ability for many priority levels to be set for different data types for improved quality of service (QoS).

Delay-tolerant network architecture

The TCP/IP protocol provides a general-purpose network- and transport-layer service for the terrestrial internet. A DTN does the same in a space environment.

The DTN architecture consists of an end-to-end message-oriented overlay known as the bundle layer. Devices implementing the bundle layer are known as DTN nodes. This layer exists above the transport (or other) layers of the network and below applications.

It provides functionality similar to the layer of gateways described in the original internet and ARPANET designs. But unlike ARPANET, the DTN bundle layer is layer-agnostic and focuses on virtual message forwarding rather than on packet switching.

The bundle layer employs persistent storage for store-and-forward. This allows it to combat network interruptions and delays. The DTN architecture uses variable-length or arbitrary-length messages instead of streams or limited-sized packets. These application data units are transformed by the bundle layer into protocol data units called bundles, which are forwarded by DTN nodes.

This communication abstraction enhances the DTN's ability to make good scheduling and path selection decisions.

In the DTN, bundle sources and destinations are identified by endpoint identifiers (EIDs), which may refer to one or more DTN nodes or endpoints. Security mechanisms are also provided in the DTN to protect the infrastructure from unauthorized use.

Traffic in delay-tolerant networks

In a DTN, traffic can be classified in three ways: expedited, normal and bulk. These traffic types move across the DTN in order of decreasing priority:

- **Expedited packets :** These are always transmitted, reassembled and verified before data of any other class from a given source to a given destination.

- **Normal traffic :** This traffic is sent after all expedited packets have been successfully assembled at their intended destination.
- **Bulk traffic :** This is not dealt with until all packets of other classes from the same source and bound for the same destination have been successfully transmitted and reassembled. In this sense, bulk bundles are sent on a “least effort” basis.

Applications of delay-tolerant networks

In addition to space communications and interplanetary networking, DTNs are also useful over terrestrial applications and more modest distances when interference is extreme, high error rates are common or network resources are severely overburdened.

Other key applications of DTNs include the following:

- military and tactical systems;
- disaster recovery networks;
- vehicular communications;
- wildlife tracking/monitoring networks;
- communication in remote or rural areas;
- underwater acoustic networks; and
- other sensor-based networks.

Hardware considerations for delay-tolerant networks

A delay-tolerant network can accommodate different kinds of wireless technologies, including radio frequency (RF), ultra-wide b and (UWB), acoustic (sonar or ultrasonic) and free-space optical technologies. Such networks overcome network problems associated with intermittent connectivity and high error rates using store-and-forward message switching.

For this, they require hardware that can store large amounts of data indefinitely, and such media must be able to survive extended power loss and system restarts. It must also be immediately accessible at any time.

For this purpose, hard drives and high-volume flash memory are ideal. Further, the data stored on these media must be organized and prioritized by software to ensure accurate and reliable store-and-forward functionality.

Short Question and Answers

1. Bandwidth.

Ans :

Bandwidth, or precisely network bandwidth, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time. That simply means that higher is the bandwidth of a network, larger is the amount of data network can be sending to and from across its path. Be careful not to confuse bandwidth with closely related terms such as the data rate and the throughput. Bandwidth is something that deals with the measurement of capacity and not the speed of data transfer.

2. Latency.

Ans :

- Being simple latency means whenever you have given input to the system and the total time period it takes to give output so that particular time period/interval is known as latency.
- Actually, latency is the in-between handling time of computers, as some of you may think that whenever some system connects with another system it happens directly but no it isn't, the signal or data follows the proper traceroute for reaching its final destination.
- Nowadays fiber optic cables are used for transmitting the signals/data from one place to another with the speed of light but obviously before reaching to the final destiny the data/signal has to pass from many checkpoints or posts and follow a proper traceroute so it takes some time to get respond from the receiver and that total round of time is known as latency.
- If you want to know the fastest possible network connection you could have from one place to another then we will suppose light as a medium because light just takes 100milli seconds(approx.) to take a round of earth. So according to the data if you let light as a medium then you can send 20 packets per second across the other sides of the world.

3. ATM.

Ans :

Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication technique that supports data-transfer rates ranging from sub-T1 speeds (less than 1.544 Mbps) up to 10 Gbps. Like other packet-switching services (Frame Relay, SMDS), ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. Instead, it relies on the inherent integrity of digital lines to ensure data integrity.

4. FDDI.

Ans :

FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the token ring protocol.

In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network (WAN).

An FDDI network contains two token rings, one for possible backup in case the essential ring falls flat.

The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps

5. Frame Relay.

Ans :

Frame Relay (frame relay) is a packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection.

It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends. It makes it more efficient than X.25, and a higher process speed achieved (it can transmit over 2,044 Mbps).

If the traffic is hefty, with a large number of small packages, its performance is more excellent than X25.

If large files transferred at high speeds, the price/performance ratio is higher in X25.

6. Net-Centric Computing.

Ans :

Meaning

Net-Centric Computing (NCC) is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network. Net-centric Computing focuses on large-scale distributed computing systems and applications that communicate through open, wide-area networks like the Internet. General examples of large-scale network-centric systems are the World-Wide Web and Computational Grids.

Net-centric computing refers to an emerging technology architecture and an evolutionary stage of client/server computing. It is a common architecture built on open standards that supports in different ways for different people to collaborate and to reach different information sources.

7. Cloud Computing.

Ans :

Cloud computing is the delivery of different computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet without direct active management by the user. Simply stating, cloud computing means storing and accessing data and programs over the internet instead of ones' computer's hard drive. Organizations are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics, and customer-facing web applications. As an example, healthcare services use the cloud to develop more personalized treatments for patients. Financial services are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to players around the world.

8. Distributed Systems.

Ans :

A distributed system is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another from any system in order to appear as a single system to the end-user. The computers that are in a distributed system can be physically together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible components, such as mainframes, personal computers, workstations, minicomputers, and so on. Common use cases of a distributed systems are electronic banking systems, massive multiplayer online games, and sensor networks.

9. Multi access networks.

Ans :

The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD).

As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link.

The Ethernet has its roots in an early packet radio network, called Aloha, developed at the University of Hawaii to support computer communication across the Hawaiian Islands. Like the Aloha network, the fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently (in Aloha, the medium was the atmosphere, while in the Ethernet the medium was originally a coax cable). The core idea in both Aloha and the Ethernet is an algorithm that controls when each node can transmit.

10. Overlay networks.

Ans :

An overlay network is a virtual or logical network that is created on top of an existing physical network. The internet, which connects many nodes via circuit switching, is an example of an overlay network.

An overlay network is any virtual layer on top of physical network infrastructure. This may be as simple as a virtual local area network (VLAN) but typically refers to more complex virtual layers from software-defined networking (SDN) or a software-defined wide area network (SD-WAN).

The overlay creates a new layer where traffic can be programmatically directed through new virtual network routes or paths instead of requiring physical links. Overlays enable administrators to define and manage traffic flows, irrespective of the underlying physical infrastructure.

11. Delay-tolerant network.

Ans :

A delay-tolerant network (DTN) is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

In such environments, the conventional internet does not work; networks are also subject to frequent disruptions, high error rates and latency of hours or even days. A DTN can overcome such challenges and reliably transmit information, ensuring dependable internet working.

Choose the Correct Answers

1. ________ specifies a complete set of rules for the connections and interactions of its physical and logical components for providing and utilizing communication services. [c]

(a) Computer Architecture
(b) Communication Architecture
(c) Network Architecture
(d) Internet Architecture

2. How many types of networks are there based on architecture? [b]

(a) one
(b) two
(c) three
(d) four

3. The ATM cell header is composed of ________ elements [b]

(a) 8
(b) 6
(c) 4
(d) All the above

4. Which one of the following cables is also known as a thin ethernet? [d]

(a) 10BaseF
(b) 10BaseT
(c) 10Base5
(d) 10Base2

5. Network in which every computer is capable of playing the role of client, server or both at the same time is called [a]

(a) peer-to-peer network
(b) local area network
(c) dedicated server network
(d) wide area network

5. Among the following which detects the error by dividing the data into the segments of equal size and then use 1's complement to find the sum of the segments. [b]

(a) parity check
(b) check sum
(c) CRC
(D) all the above

7. Among the following which client does the majority of data processing on its own, and depends on the server only a little. [a]

(a) thin client
(b) thick client
(c) hybrid client
(d) all the above

8. The expensive software and additional computing power can be shared by the computers in a network with the help of ________ servers. [b]

(a) File server
(b) application server
(c) database server
(d) print server

9. Which one is an error control protocol? [d]

(a) Stop and Wait
(b) Go Back N
(c) Selective Repeat
(d) All of the above

10. In class A IP address the first 8 bits represent ________. [a]

(a) Network ID
(b) Host ID
(c) Both a and b
(d) None of the above

Fill in the Blanks

1. ________ is the organization and arrangement of different network devices (i.e., the clients such as PCs, desktops, laptops, mobiles etc.) at both physical and logical levels in order to fulfil the needs of the end user/customer.

3. The________ referred to here are the individual devices linked together directly, having equal responsibilities and equal powers without the presence of any central authority.

3. ________ measures of the amount of data that can be sent and received at any instance of time.

4. ________ is a cell-based fast-packet communication technique.

5. ________ is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network

6. The more general name for the technology behind the Ethernet is ________.

7. An ________ is a virtual or logical network that is created on top of an existing physical network.

8. A ________ is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content.

9. ________ server is used to co-ordinate the interaction between users, documents and applications. The data can be used in the form of audio, video, binary, text or graphics.

10. A ________ is a network that's designed to operate effectively in extreme conditions and over very large distances, such as with space communications.

Answers

1. Network architecture
2. Peers
3. Bandwidth
4. Asynchronous Transfer Mode (ATM)
5. Net-Centric Computing (NCC)
6. CSMA/CD
7. Overlay network
8. CDN
9. Message server
10. Delay-tolerant network (DTN)

UNIT II

SWITCHING :

Circuit-Switched Networks, Datagram Networks, Virtual-Circuit Networks, Message Switched Networks, Asynchronous Transfer Mode: Evolution, Benefits, Concepts, Exploring Broadband Integrated Services Digital Network, Layer and Adaptation Layer

2.1 Switching

2.1.1 Circuit-switched Networks

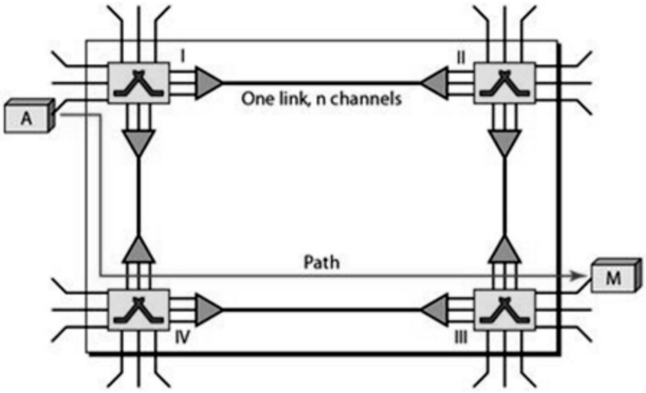
Q1. Explain about circuit switched networks.

Ans : **(Imp.)**

A network consists of a set of switches that are connected by the physical links commonly known as Circuit-Switched Network.

- Whenever one device communicates with another device then a dedicated communi- cation path is established between them over the network.
- There is only a dedicated channel on each link used by each connection. Also, each link can be easily divided into n channels by using the TDM(Time Division Multiplexing) or FDM(Frequency Divison Multiplexing) technique.
- The Circuit Switching technique is mainly used in the public telephone network for voice communication as well as for data communication.
- Data communication is less efficient than voice communication.
- The Circuit switching technique mainly takes place at the physical layer.
- In Circuit-switched networks, the data transfer mode mainly involves a dedicated end-to-end connection. Until the end of the communication, this dedicated path is maintained. After the communication is over the link is released.

The following figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.Phases in



Circuit Switching

In order to transfer data using Circuit switching there is a need to establish a circuit (these circuits can either be permanent or temporary) so that data transfer can take place smoothly. Given below are three phases that are used in Circuit Switching for actual communication:

1. Setup Phase
2. Data Transfer Phase
3. Teardown Phase

1. Setup Phase

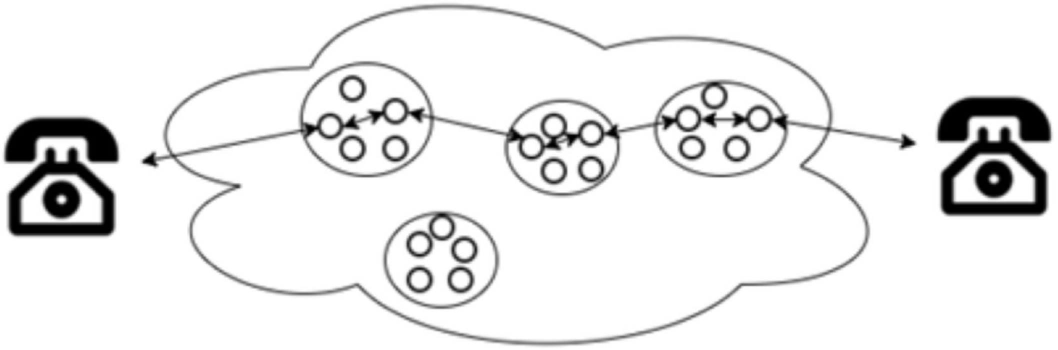
It is the first phase of the Circuit switching technique and in this, there is an establishment of the circuit that simply means a dedicated link is established between the sender and the receiver with the help of several switching centers or nodes.

2. Data Transfer Phase

After the establishment of the circuit, the connection is established which means that data transfer can take place between sender and receiver.

3. Teardown Phase

On the completion of communication between the sender and receiver the circuit disconnects. In order to disconnect a signal is sent either by the sender or receiver



One of the best examples of Circuit switching is a telephone. Suppose there are two persons Person A and Person B; they both want to communicate with each other and located at a distance far from each other.

Person A makes a call to Person B this phase is the setup phase of circuit switching. After the establishment of the connection and after call pick up by Person B; they both can communicate with each other. This is the data transfer phase of Circuit switching

Once the communication is complete one of them can cut the call or break the connection. This is a teardown phase.

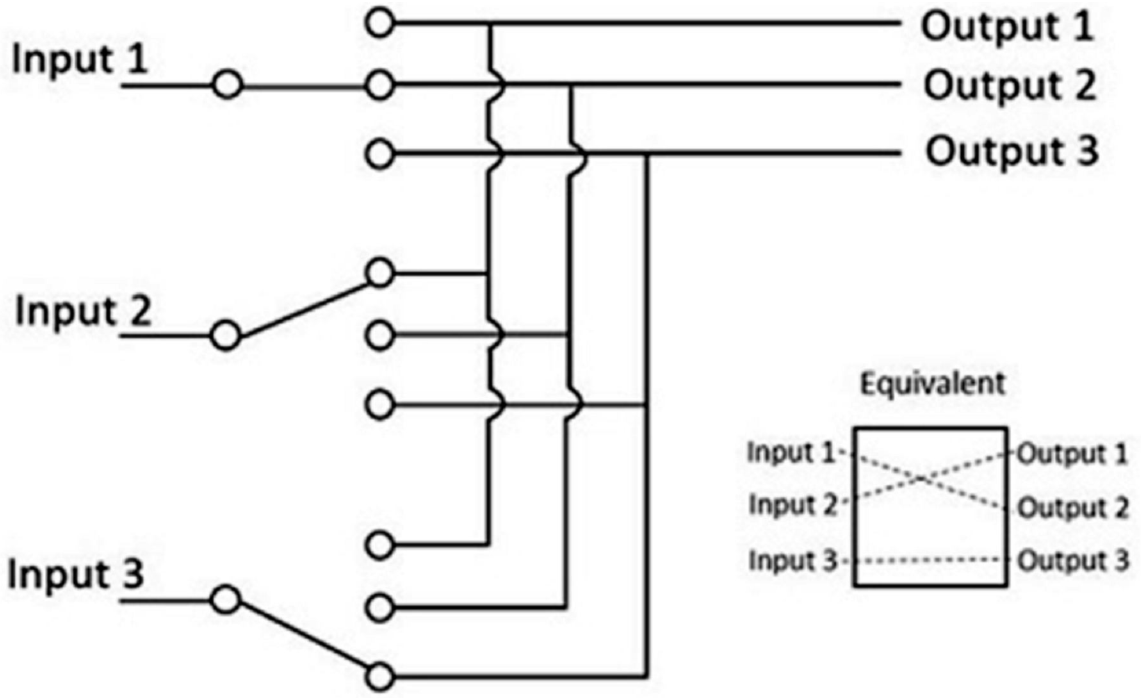
Circuit Switching can be further classified into two:

1. Space-Division Switching
2. Time-Division Switching

1. Space Division Switching

The paths in a circuit are separated from each other, spatially in space division switching. Though initially designed for analog networks, it is being used for both analog and digital switching. A Crosspoint switch is mostly referred to as a space division switch because it moves a bit stream from one circuit or bus to another.

The switching system where any channel of one of its incoming PCM highway is connected to any channel of an outgoing PCM highway, where both of them are spatially separated is called the Space Division Switching. The Crosspoint matrix connects the incoming and outgoing PCM highways, where different channels of an incoming PCM frame may need to be switched by different Cross points in order to reach different destinations.



Though the space division switching was developed for the analog environment, it has been carried over to digital communication as well. This requires separate physical path for each signal connection, and uses metallic or semiconductor gates.

Advantages

Following is the advantage of Space Division Switching -

- It is instantaneous.

Disadvantages

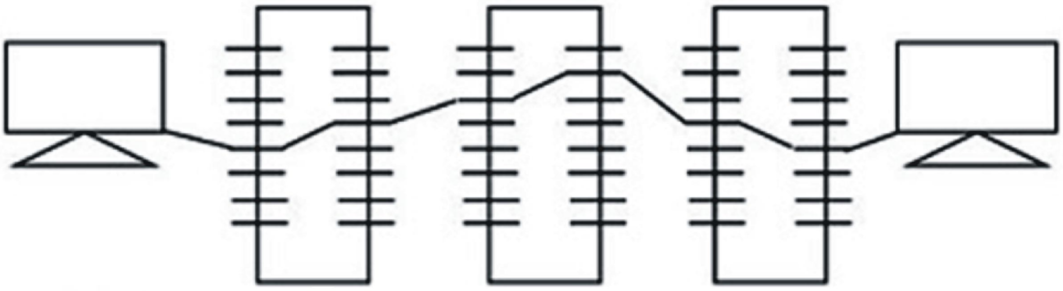
- Number of Cross points required to make space-division switching are acceptable in terms of blocking.

2. Time Division Switching

Time division switching comes under digital switching techniques, where the Pulse Code Modulated signals are mostly present at the input and the output ports. A digital Switching system is one, where the inputs of any PCM highway can be connected to the outputs of any PCM highway, to establish a call.l

The incoming and outgoing signals when received and re-transmitted in a different time slot, is called Time Division Switching. The digitized speech information is sliced into a sequence of time intervals or slots. Additional voice circuit slots, corresponding to other users are inserted into this bit stream of data. Hence, the data is sent in time frames.

The main difference between space division multiplexing and time division multiplexing is sharing of Cross points. Crosspoints are not shared in space division switching, whereas they can be shared in time division multiplexing, for shorter periods. This helps in reassigning the Crosspoints and its associated circuitry for other connections as well.



Time division switches use time division multiplexing, in switching. The two popular methods of TDM are TSI (Time and Slot Interchange) and TDM bus. The data sent at the transmitter reaches the receiver in the same order, in an ordinary time division multiplexing whereas, in TSI mechanism, the data sent is changed according to the ordering of slots based on the desired connections. It consists of RAM with several memory locations such as input, output locations and control unit.

Both of the techniques are used in digital transmission. The TDM bus utilizes multiplexing to place all the signals on a common transmission path. The bus must have higher data rate than individual I/O lines. The main advantage of time division multiplexing is that, there is no need of Crosspoints. However, processing each connection creates delay as each time slot must be stored by RAM, then retrieved and then passed on.

Time Division Multiplexing

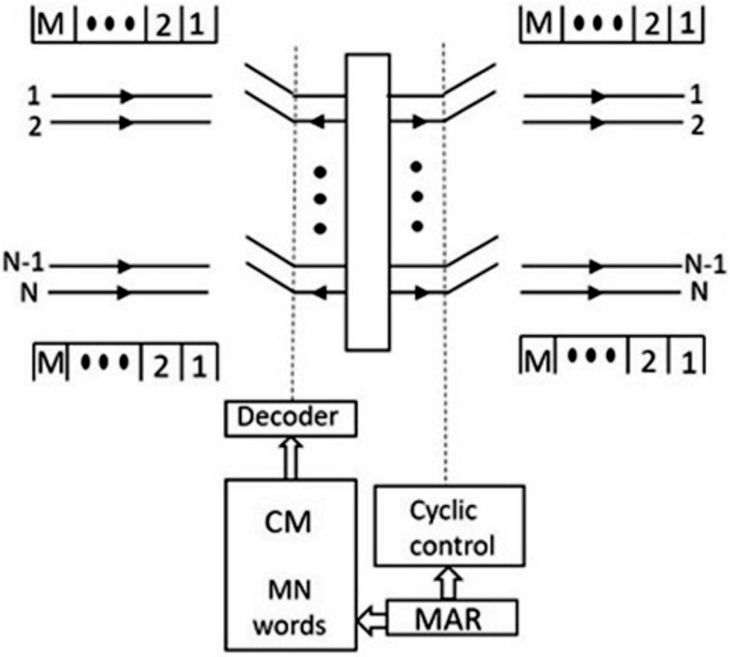
When the transmission of data or signals is done in digital means, using the limited number of resources available, then the Time Division Multiplexing is used for the transmission of such data. Multiplexing is the process in communication, which merges two or more signals at its input into a single output, which when de-multiplexed, offers all those signals separately as they were.

The Multiplexers are broadly classified as Analog and Digital, where the Time Division Multiplexing comes under Digital Multiplexing. There are two types of TDM called as Synchronous and Asynchronous TDM.

Time Division Space Switching

Time division switches may also employ space division switching techniques, whereas an appropriate mixture of both time and space division switching is advantageous in various circumstances.

A Time division space switch takes outputs of several time-division switches (say, TSI switches) which are then given as inputs to space division switches. This means that one of the two similar outputs produced by a TDM switch, can be selected by space switch to deliver to another output path which reduces the number of Crosspoints. The model of time division space switch is as shown in the following figure.



The interchange of time slots is not possible in time division switching, as the incoming time slot transfers the data to its dedicated output time slot only. Hence, time multiplexed switches do not provide full availability.

A time multiplexed Time Division Space Switch can be configured around a space array, which has M input horizontals and N output verticals. If both inputs and outputs are equal, M=N the switch leads to non-blocking. If inputs are greater than outputs; for concentrating switch we have M>N and if the outputs are higher, the switch expands gathering one more connection. In every time slot, one logic gate per vertical if M>N, or one logic per horizontal if M>N is enabled for one-to-one connections.

In every time slot, up to N or M samples are switched simultaneously. Because of the parallel transfer of N or M data samples in each time slot, a large number of channels can be multiplexed per input line. If along with multiplexing for N control memory modules, full availability has to be achieved, one should opt for time division time multiplexing technique.

Q2. Explain the benefits and Limitations of Circuit Switching.

Ans:

Advantages of Circuit Switching

Given below are some of the benefits of Circuit Switching:

1. **Offers Dedicated Transmission**

   As there is a dedicated link between the sender and the receiver. Thus Circuit-Switched network provides a guarantee of dedicated transmission.

2. **No Delay in Transmission**

   There is a dedicated path between sender and receiver thus there are no chances for the delay.

3. The Circuit Switching technique is best for long transmission because it facilitates a dedicated link between sender and receiver.

Disadvantages of Circuit Switching

There are some drawbacks of Circuit Switching and these are as follows:

- One of the main disadvantages of Circuit switching is that as there is a dedicated path between sender and receiver; thus this path is received for these two particular devices and cannot be used by any other device.
- There is a need for more bandwidth as a dedicated path requires more bandwidth.
- Utilization of resources is not done properly as resources are allocated to a connection for the entire duration and thus became unavailable for all other connections.
- It becomes inefficient in the case if the connection is established between sender and receiver but there is no data transfer between them.
- Sometimes it takes a long time to establish the connection between sender and receiver.
- As there is a dedicated path between sender and receiver; thus, this technique is expensive.

2.1.2 Datagram Networks

Q3. Explain about Datagram Networks.

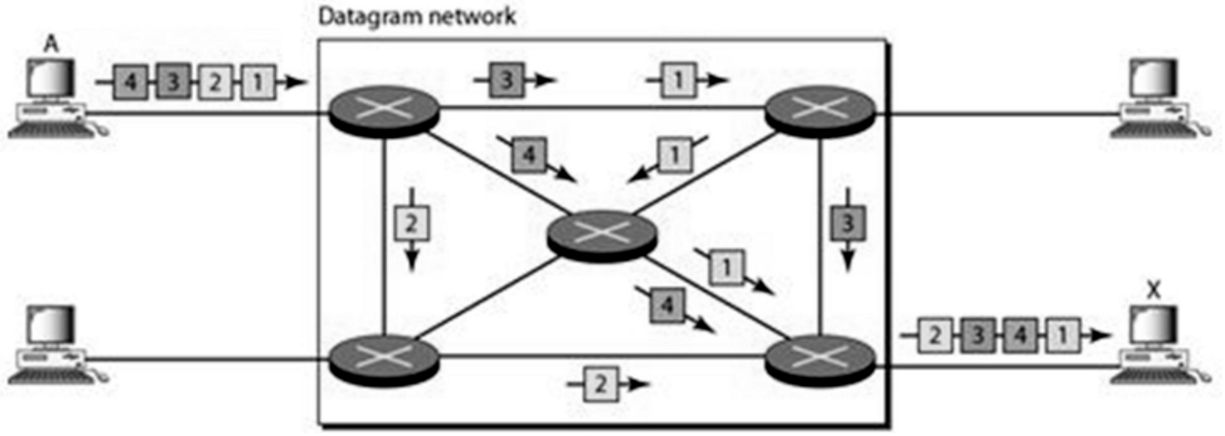
Ans: **(Imp.)**

Introduction

It is a packet-switching technique in which each packet, known as a datagram, is treated as a separate entity. Each packet carries destination information, which the switch uses to route the packet to the correct destination. There is no need to reserve resources because there is no specified channel for a connection session. As a result, packets contain a header including all of the destination's information. The intermediate nodes examine the header of a packet and choose an appropriate link to a different node closer to the destination.

Resources in datagram networks are allocated on a First Come First Serve (FCFS) basis. When a packet arrives at a router, it must wait if other packets are being processed, regardless of its source or destination.

The diagram below displays datagram packets sent from host H1 to host H2. The four datagram packets with the labels A, B, C, and D are all parts of the same message each being routed individually through a different route. The message's packets arrive out of sequence at their destination. In order to recover the original message, it is H2's obligation to reorder the packets.



In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks.

- **Routing Table**

  In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.

- **Destination Address**

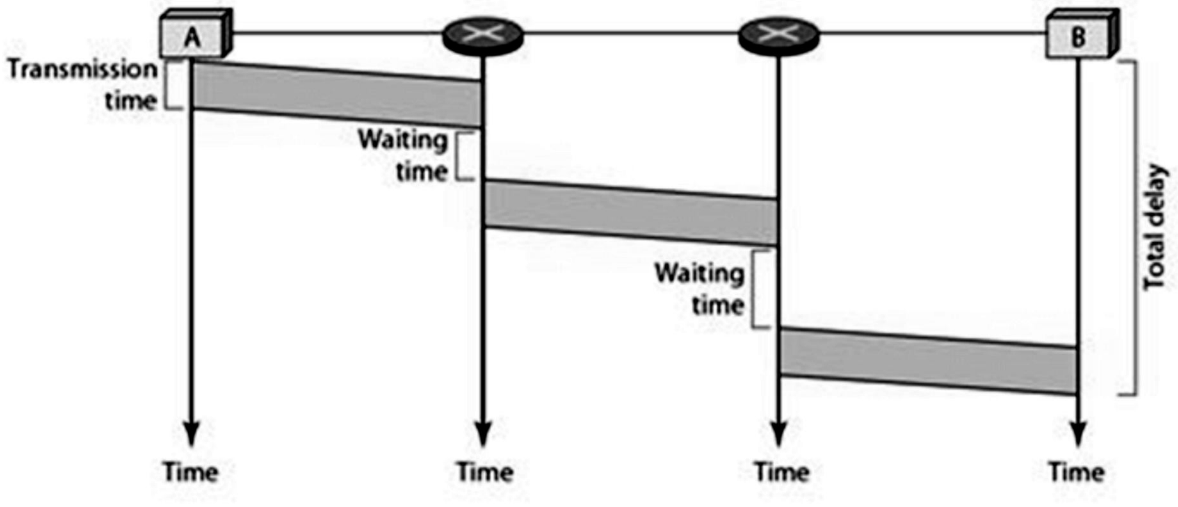
  Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

- **Efficiency**

  The efficiency of a datagram network is better than that of a circuit-switched network. Resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

- **Delay**

  There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message. The following figure gives an example of delay in a datagram network for one single packet.



The various important points related to Datagram Networks.

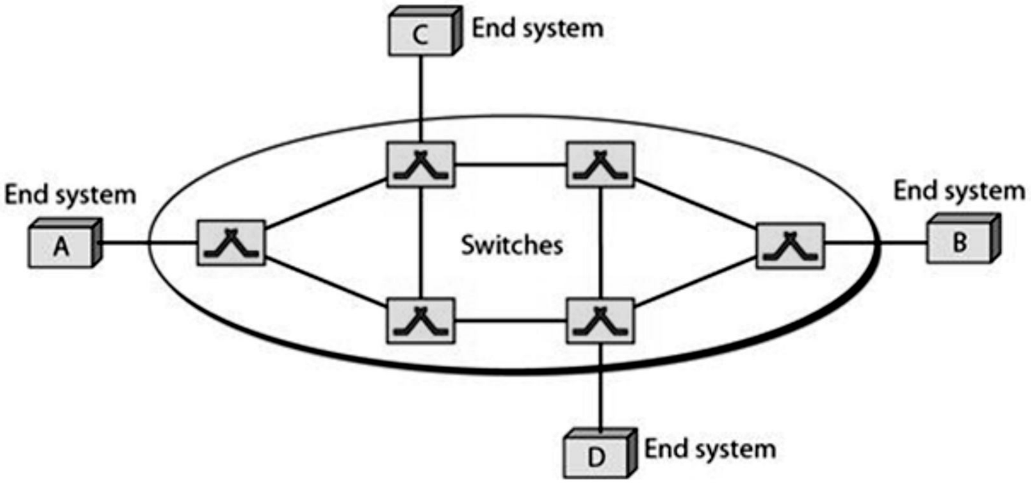
- At the network layer, datagram networks are computer networks that provide a connectionless service.
- Since there is no specific path for a connection session, there is no need to reserve resources.
- Datagram networks are implemented in routers in the network core and end systems.
- The order in which the packets were sent does not necessarily reflect the order in which they arrive at their destination.
- Since routing tables on routers change dynamically, all packets are free to go through any intermediary router chosen at the time.
- Datagram networks are unreliable because their connectionless nature causes data packets to arrive at their destination out of the sequence as they were sent from the source.
- Since there is no need to reserve resources every time an application needs to communicate, datagram networks are always affordable and straightforward to install.
- Every packet must be associated with the complete address of the destination site (header) since every packet in datagram networks is free to choose any path.
- Route changes and packet loss are possible with malfunctioning routers.
- It is typically utilized in IP networks, which support data services like the internet.

Advantages

- Greater line utilization efficiency.
- Priorities are used.
- When traffic becomes heavy some calls are blocked.
- Errors are corrected by retransmission.
- Cost of intermittent data communication is reduced.

Disadvantages

- Delay.
- Overall packet delay can vary substantially.
- More processing required at the node.



Addressing

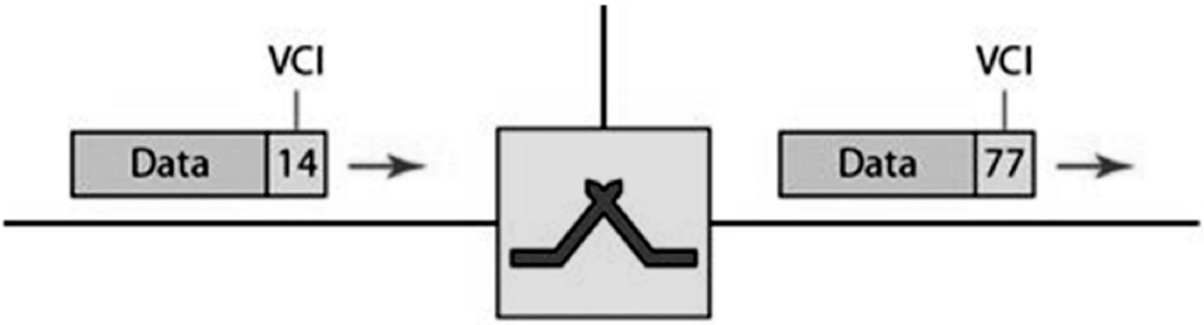
In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing

A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope. It is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI. The following figure show how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCIs.



Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

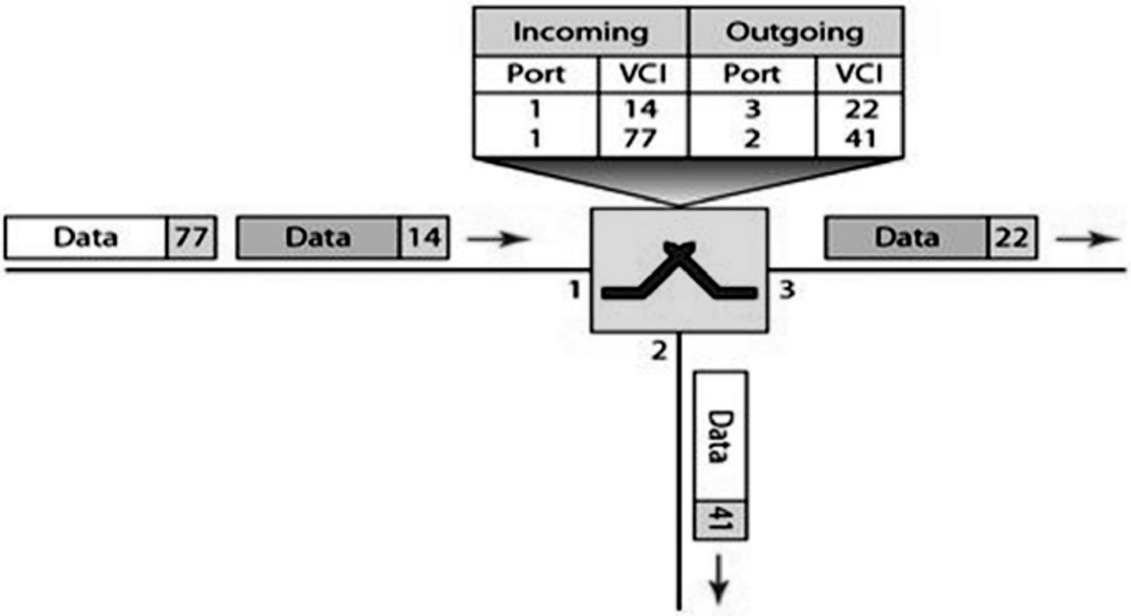
In the teardown phase, the source and destination inform the switches to delete the corresponding entry.

Data transfer occurs between these two phases.

Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits.

The following figure shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

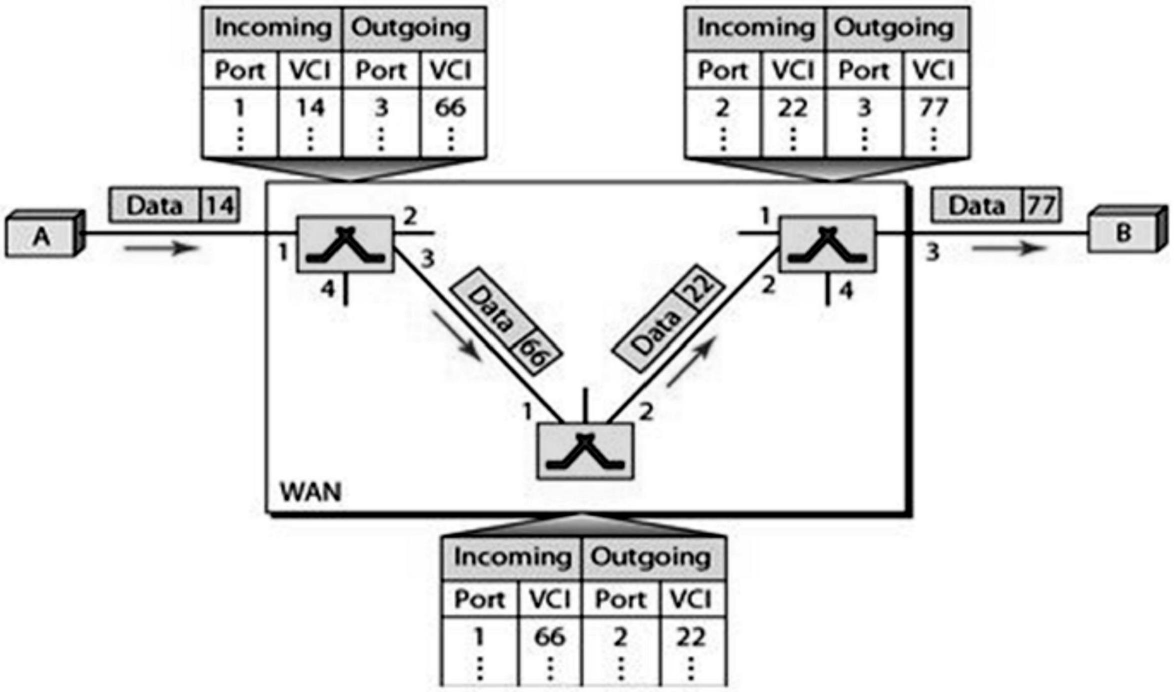


Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

Setup Request: A setup request frame is sent from the source to the destination. The following figure shows the process.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22
⋮	⋮	⋮	⋮

(a) Source A sends a setup frame to switch 1.

(b) Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. The switch, in the setup phase, acts as a packet switch and it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.

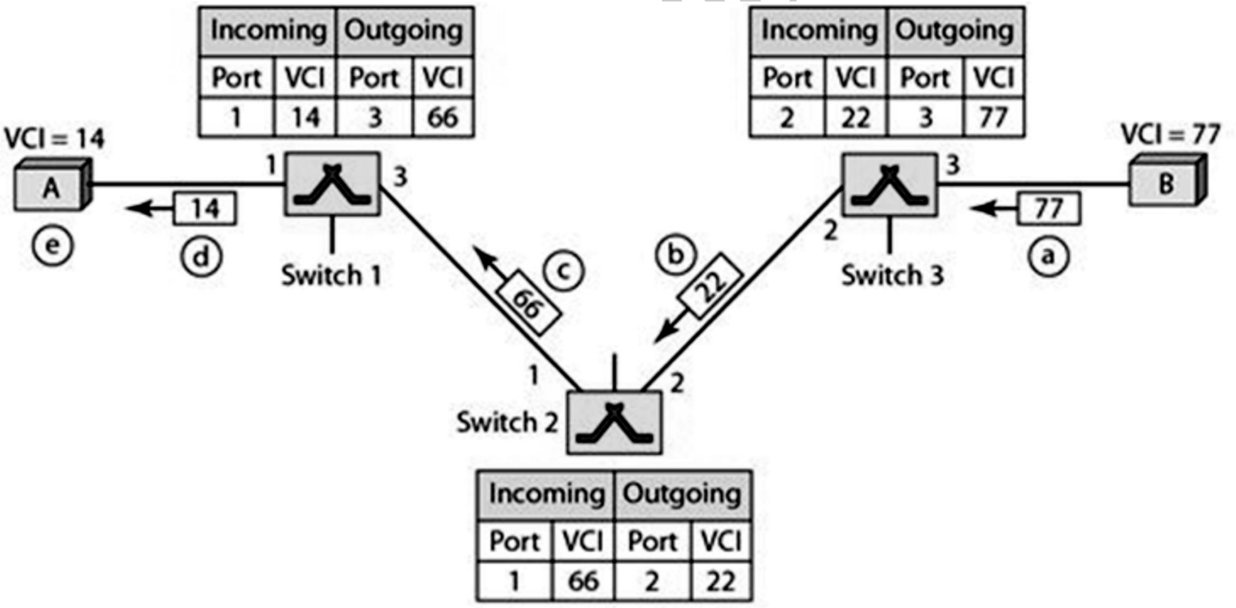
(c) Switch 2 receives the setup request frame. The same events happen here as at switch 1 and three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

(d) Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

(e) Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and no other sources.

Acknowledgment

A special frame, called the acknowledgment frame, completes the entries in the switching tables. The following figure shows the process.



(a) The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.

(b) Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

(c) Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.

(d) Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

(e) The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency

- Resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays.
- There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it.

Advantages

- No of bit required in the header is much smaller than no required to provide full destination address.
- Resources can be allocated during connection setup.
- It follows fast processing and forwarding of packets.

Disadvantages

- Connection setup is not possible.
- In the case of fault occurs in the network, all affected connections must be setup again.
- The switches in the network need to maintain information about the flows they are handling.

Q4. Write Differences between Virtual Circuits & Datagram Networks.

Ans: **(Imp.)**

S.No.	Basis of comparison	Virtual Circuits	Datagram Networks
1.	Definition	Virtual Circuits are also known as connection-oriented switching. Virtual circuit switching establishes a predetermined path before messages are sent. to the correct destination.	It is a packet-switching technique in which each packet, known as a datagram, is treated as a separate entity. Each packet carries destination information, which the switch uses to route the packet
2.	Connectivity	It is connection-oriented.	It is connectionless.
3.	Path	In these networks, the path taken by the initial data packet between the source and destination nodes is allocated. All subsequent data packets sent between them will take the same path. different paths to their destination.	Since each datagram is treated independently, there is no fixed dedicated path for data transfer. The intermediate routers use dynamically updating routing tables to route each datagram. Therefore, two subsequent packets from the source may travel entirely

4.	**Header**	Since they are all part of the same virtual circuit, all packets that make up a message have the same header information.	Even though they are part of the same communication, the separate datagram packets have different header information.
5.	**Phases**	Transmission is performed in three steps: setup, data transfer, and teardown.	There are no such communication phases.
6.	**Complexity**	In comparison to a datagram network, a virtual circuit is less complex.	However, compared to the virtual circuit, datagram networks are more complex.
7.	**Cost**	Installation and maintenance costs for virtual circuits are higher.	Networks using datagrams are much easier to set up and maintain.
8.	**Resource Utilization**	All resources, including CPUs, band width, and buffers, are reserved before transmission. All data packets use the same resources, which are only released when the transmission is complete.	Before the transmission starts, no initial resource allocation is made for the individual packets. The resources are distributed on demand on a First-Come First-Serve (FCFS) basis when a packet arrives at a router.
9.	**Reliability**	In comparison to the Datagram network, Virtual Circuits are more reliable for data transmission due to the defined path and assurance of fixed resources.	On the other hand, datagram networks are less reliable than virtual circuits since they allocate resources dynamically and follow dynamic paths.
10.	**Addressing**	During setup, the addressing and route are decided. As a result, each packet just includes the VC number.	The complete source and destination addresses are included in each datagram packet.
11.	**Application**	Virtual Circuits are implemented in networks using Asynchronous Transfer Mode (ATM) communi-cations, such as when placing phone calls.	User Datagram Protocol (UDP) typically serves as the framework for datagram communication. In IP networks, they are used.

2.1.3 Message Switched Networks

Q5. What is Message Switching? Explain.

Ans: **(Imp.)**

Message Switching is a network switching strategy in which data or message is transmitted entirely from the source to the destination node, one hop at a time. Every intermediary switch in the network stores the entire message during message routing.

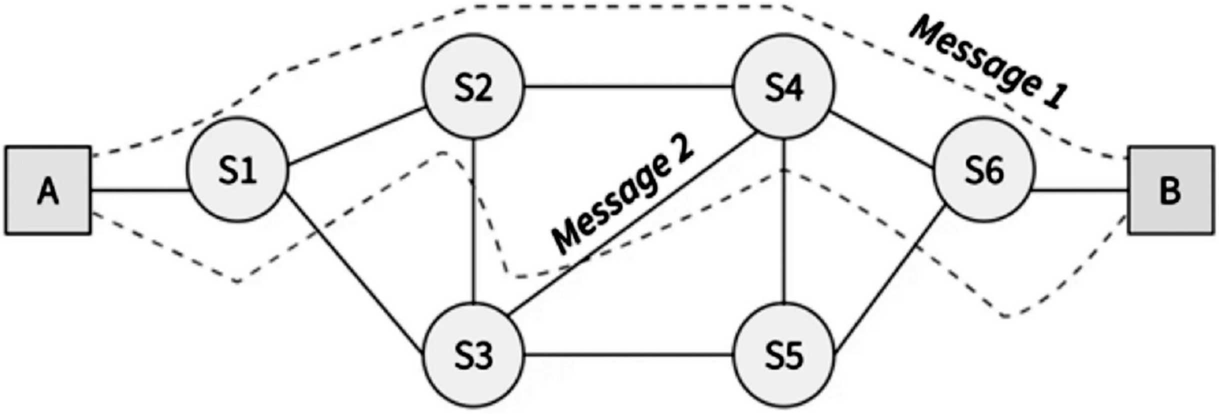
If all of the network's resources are used up, or the network becomes blocked, the message-switched network stores and delays the message until sufficient resources are available for effective transmission. Message switching served as an adequate replacement for circuit switching before the development of packet switching. The first applications of it were in data transmissions via telex networks and paper tape relay systems. Although packet switching has completely supplanted message switching, ad hoc sensor networks, military networks, and satellite communications networks still use the technique.

The source node and destination nodes are not directly coupled in message switching. Instead, intermediary nodes (mostly switches) are in charge of transmitting messages from one node to the next. As a result, every intermediary node in the network must retain each message before retransmitting them one at a time as appropriate resources become available. Messages are retained indefinitely if the resources are not available. This process is referred to as store and forward. Every message should include a header, which generally contains routing information such as the source and destination, expiry time, priority level, and so on.

Each switching node in a message switching network must have enough storage to buffer messages because message switching treats each message as a single complete entity. So if the message size exceeds the storage capacity of the switch, then the message is strictly discarded. This is one of the significant disadvantages of using these switching methods.

The figure below explains how messages are transferred from sender to receiver in the Message Switching networks.

In the figure Message 1 follows the path A->S1->S2->S4->S6->B, while the Message 2 follows A->S1->S2->S3->S4->S6->B. This is due to the fact Message switching uses dynamic routing.

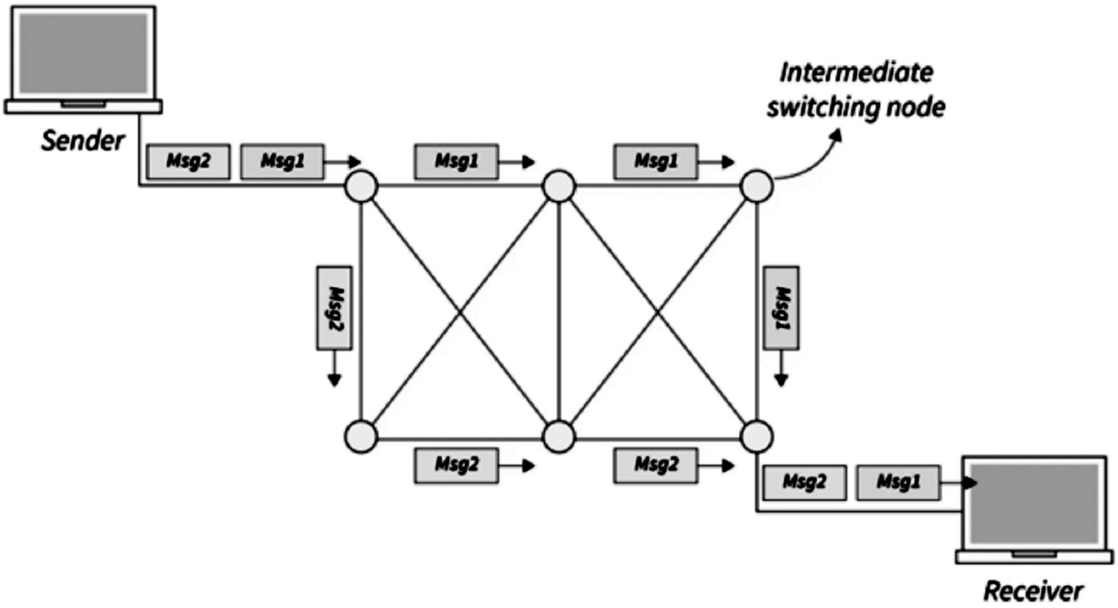


Process of Message Switching

Message switching treats each message as a separate entity. The sender node adds the destination address to the message before sending the message. Then the message is completely delivered to the next intermediate switching node. The intermediate node stores the complete message, checks for transmission errors, validates the destination address and then forwards it to the next node. This process is repeated until the message reaches its destination.

If the needed outgoing circuit is busy, the incoming message is not discarded by the switching node. Instead, it is queued for that route and retransmitted when the required route becomes available. This is referred to as a store and forward network.

The diagram given below illustrates the complete process of Message Switching.



Characteristics

1. Store and Forward

In a Message Switching network, the sender and receiver are physically not connected to each other. As a result, intermediate nodes between sender and receiver are primarily in charge of forwarding the message to the next node in the network.

Thus, intermediate nodes must have storage capacity to transfer the message because any message will only be transferred if the next node and the link between them are accessible to connect; otherwise, this message will be retained indefinitely.

A store-and-forward switch will thus forward a message only if adequate resources are available and the following node is ready to accept the data. The procedure is repeated until the data is transferred to the destination node. As a result, it is known as the store-and-forward property. Previously, the store-and-forward property was used in telegraph message switching facilities.

2. Message Delivery

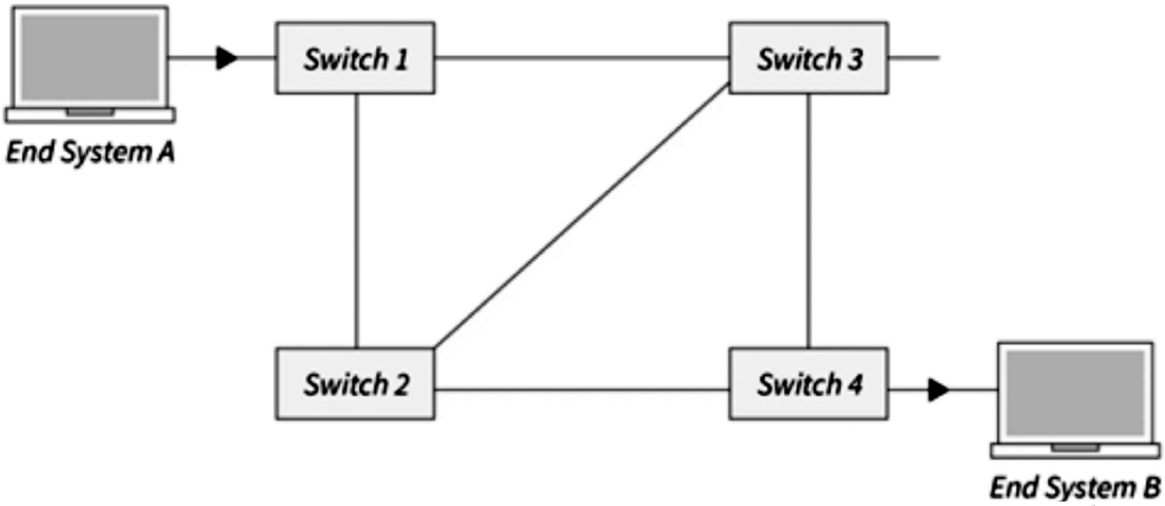
This implies encapsulating the complete information in a single message and sending it from the source to the destination node. Each message must have a header with message routing information, such as the source and destination.

3. Delay in Message Switching

(i) A message switched network comprises store-and-forward switches linked together by trunks. A single trunk is usually enough to connect two switches.

(ii) We can provide multiple trunks to boost reliability. Every switch has a storage unit where all incoming messages are momentarily held before being transmitted to another switch.

A network trunk is a communications link or link that is designed to transport multiple signals at the same time to offer network access between two points.



(iii) The store-and-forward service operates similarly to the telegram service. A message is forwarded from switch to switch with the destination address till it reaches the destination.

(iv) As illustrated in Fig, assume that end system A wishes to transmit a message to end system B. A sends its message to entry switch 1 coupled with the destination's and its own addresses. The addresses are contained in the message's header.

(v) The message is accepted by Switch 1, and the destination address is examined. Each node maintains its routing table. This routing table contains entries representing destination nodes and the switch's corresponding outgoing trunks. Every trunk has its queue.

(vi) As we can reach the destination node via multiple routes, the decision to send the message to a specific next switch is based on the expected delay in its queue. Assume the message from A is queued for node 2.

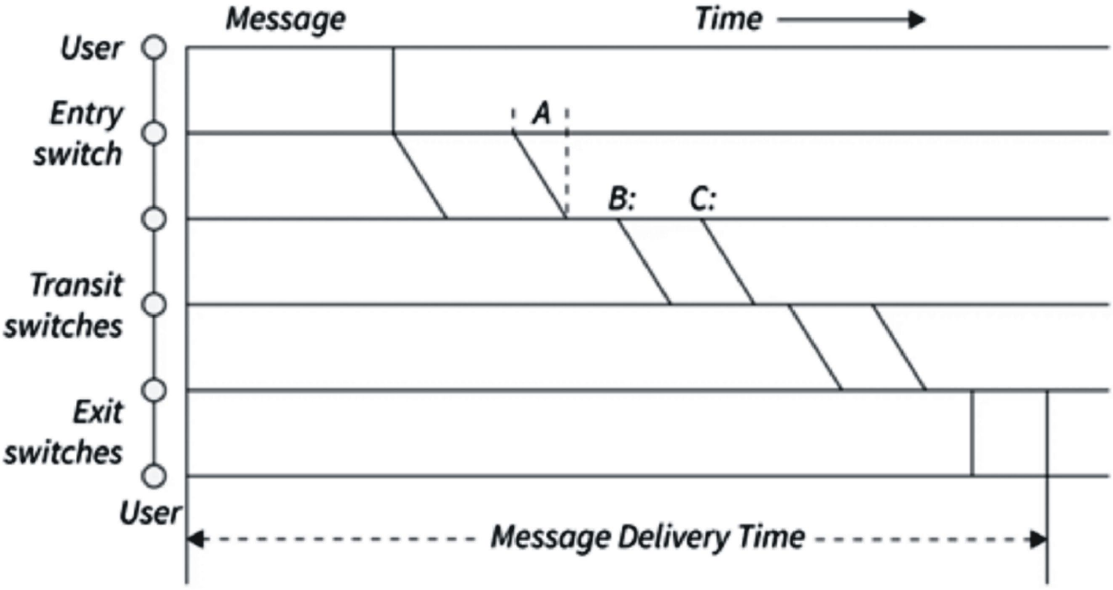
(vii) The message received at switch 2 is added to a queue of messages waiting to be transmitted to switch 4. When its turn comes, the message is routed to switch 4, which forwards it to the intended recipient.

(viii) Some of the fundamental characteristics of store-and-forward message switching, which are the main reasons for delay in message switching networks, are as follows:

- The store-and-forward service is unidirectional. The network does not send confirmation to the source after the message is delivered. Suppose end system B is required to send an acknowledgment to the message received from A. In that case, the network treats the acknowledgment like any other message and includes the destination and source addresses.
- The network may use an error control mechanism for message transfer from switch to switch. The message may be appended with error-checking bits, and if an error is detected, the receiving switch may request the retransmission of the message from the sending switch. As a result, the sending switch must retain a copy of the message until an acknowledgment is received.

- As the message is buffered at the switch at each transmission stage, each switch-to-switch transfer is a separate operation. The trunks can operate at a variety of data rates. The end systems at the source and destination can operate at different data rates.
- The network treats each message as a distinct entity in message switching; therefore, each message's destination and source addresses are repeated.

(ix) Delay in delivery. The time diagram for routing a message through a message switching network is shown in Figure. The message travels through the entry switch, two transit switches, and ultimately the exit switch to reach its destination.



A : switch to switch propagation time

B : switch Delay

C : Message transmission time

So the total time in message delivery is calculated by the sum of the following components:

- The Switch delay.
- Switch To switch propagation delay.
- Message Transmission Time.

Advantages

- Message switching reduces network traffic congestion because it can store messages for which no communication channel is available.
- Message broadcasting takes far less bandwidth than circuit switching.
- Unlike circuit switching, it does not require the physical connection of source and destination devices.
- It is possible to include priority in the messages because they are transmitted using a store and forward approach.

- We can alter the size of the message sent across the network. As a result, it handles any amount of data.
- Data channels are shared across connected devices, improving the available bandwidth's efficiency.
- Message switching systems can send a single message to several destinations; however, this capability is not available in circuit switching.

Disadvantages

- Since message length is unbounded, each switching node must have enough storage to buffer messages.
- Message switching cannot be employed for real-time applications since storing messages adds time to the process.
- The message switching method does not establish a dedicated path between the devices. There is no direct relationship between the sender node and the receiver node, hence communication is not reliable.
- Message-switched networks are highly sluggish since processing occurs in every node, resulting in poor performance.
- People are generally unaware of whether messages are correctly sent since the system is so complex. This could lead to difficulties in social relationships.

Applications

- In telegraph message switching centers, the store-and-forward approach was used.
- Although many essential networks and systems today are packet-switched or circuit-switched networks, their delivery mechanisms might be message-based.
- For instance, In most electronic mail systems, the delivery mechanism is based on message switching, whereas the network is circuit-switched or packet-switched.

2.2 Asynchronous Transfer Mode

2.2.1 Evolution

Q6. Write about how ATM evolved.

Ans:

The concept of ATM was developed at first hand itself. In the 1990s, the mobile data carrier speed along with the internet speed saw a boom in the transfer rate. On the other hand, other internet technologies such as voice call and video calls had also started to come into the play. So, in a nutshell, it was not only the internet world but also the telephony world which were converging into each other. Thus networking QoS factors such as latency, jitter, data rate, real-time data delivery, etc., became more important.

It is an International Telecommunication Union - Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. Each cell is 53 bytes long – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with end-to-end quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

2.2.2 Benefits

Q7. Write the benefits and Drawbacks of ATM network.

Ans: **(Imp.)**

Benefits

Following are the benefits or advantages of Asynchronous Transfer Mode (ATM):

- It is optimized to transport voice, data and video i.e. single network for everything. It is used for mixed traffic, real-time and non real time traffic types.
- It is easy to integrate with LAN, MAN and WAN network types i.e. seamless integration.
- It is QoS oriented and high speed oriented.
- It enables efficient use of network resources using bandwidth on demand concept.
- It uses simplified network infrastructure.

Drawbacks

Following are the disadvantages of Asynchronous Transfer Mode (ATM):

- Overhead of cell header (5 bytes per cell)
- Complex mechanisms are used to achieve QoS.
- Congestion may cause cell losses
- ATM switch is very expensive compared to LAN hardware. Moreover ATM NIC is more expensive compared to ethernet NIC.
- As ATM is connection oriented technology, the time required for connection setup and tear down is larger compare to time required to use it.

2.2.3 Concepts

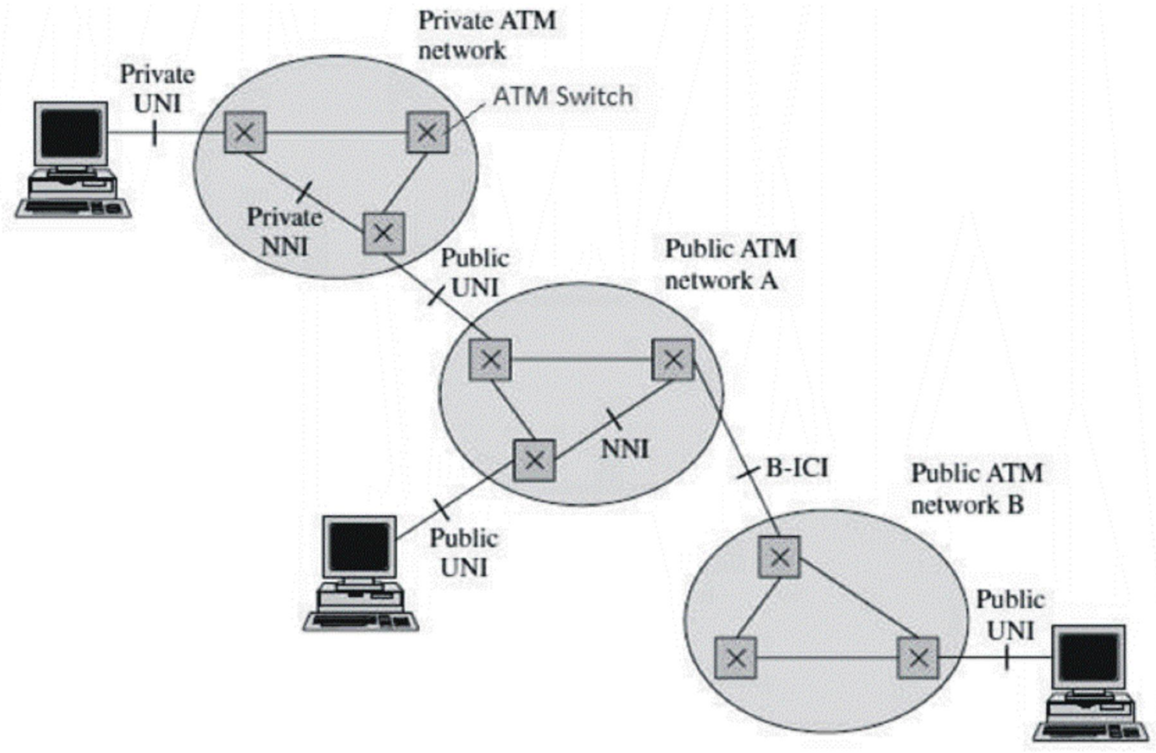
Q8. What is Asynchronous Transfer Mode (ATM)? Expalin.

Ans: **(Imp.)**

Introduction:

ATM stands for Asynchronous Transfer Mode. ATM technology uses ATM cells for data transmission between source and destination. ATM cell uses fixed size of 53 bytes which consists of header (5 bytes) and data (48 bytes). It is behind the success of B-ISDN used for voice/data/video transportation.

ATM transmits cells only when there is data to be transmitted unlike STM (Synchronous Transfer Mode) where bandwidth is assigned periodically like TDM. ATM is connection oriented which uses virtual packet switching. Multiple logical connections are multiplexed over single physical connection.



The full form of the ATM is Asynchronous Transfer Mode. Asynchronous Transfer Mode is a switching technique and time division multiplexing (TDM) is used by ATMs for data communication. Time-division multiplexing (TDM) is a method in which multiple data

Importance

1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).
2. Telephone networks support a single quality of service and are expensive to boot.
3. Internet supports no quality of service but is flexible and cheap.
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM):

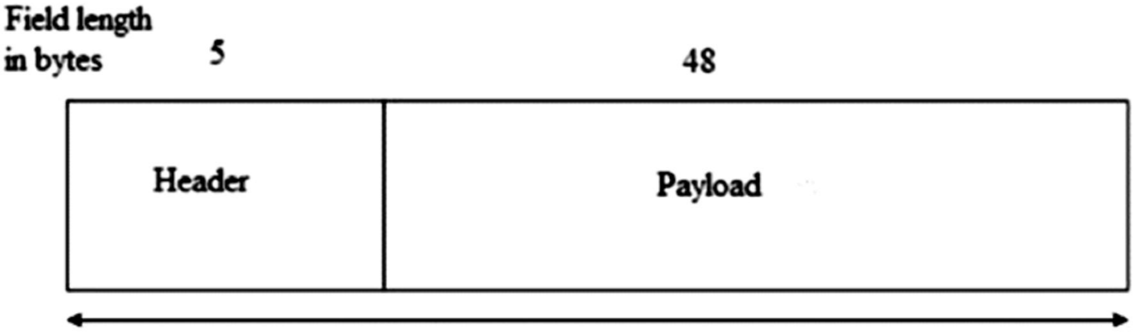
It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. Each cell is 53 bytes long – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with end-to-end quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use “Packet” or “cell” Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

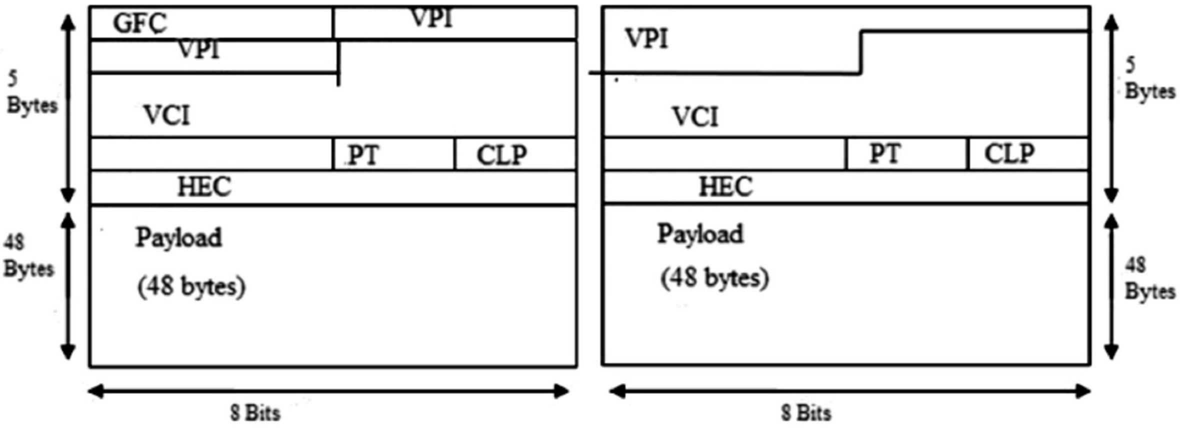
ATM Cell Format

As information is transmitted in ATM in the form of fixed-size units called cells. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Asynchronous Transfer Mode can be of two format types which are as follows:



UNI Cell Format NNI Cell Format

UNI Header: This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

1. **NNI Header**

   Is used for communication between ATM switches, and it does not include the Generic Flow Control (GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

   Working of ATM:

   ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

ATM vs DATA Networks (Internet) :

- **ATM is a "virtual circuit" based**

  The path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.

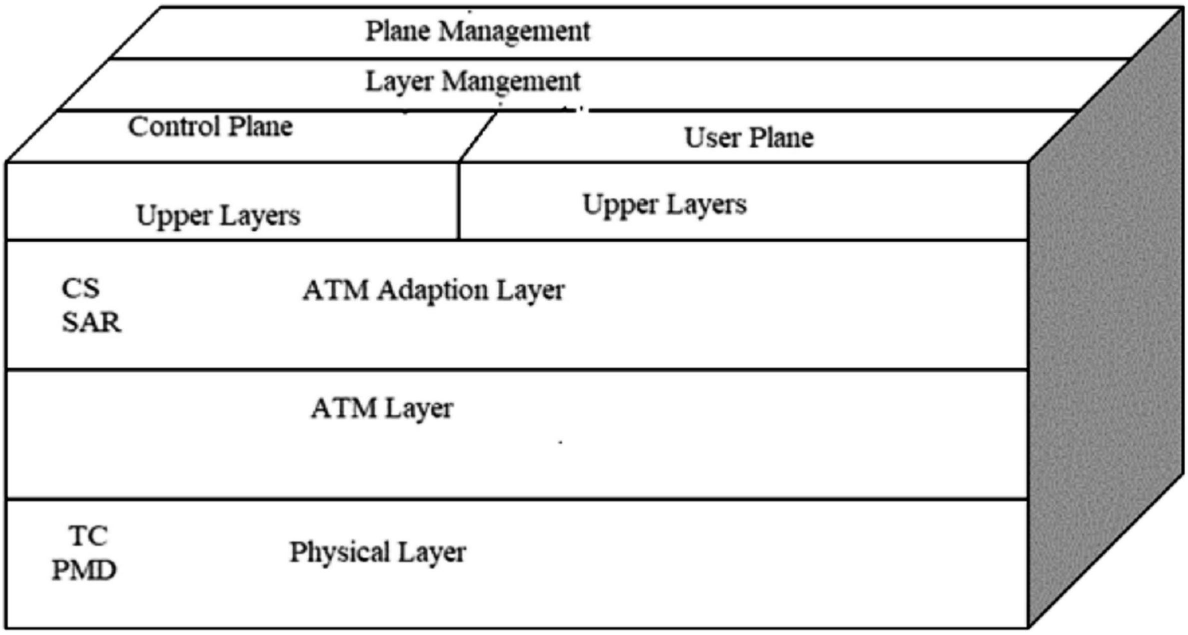
- **ATM Cells**

  Fixed or small size and Trade off is between voice or data. While IP packets are of variable size.

- **Addressing**

  ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.

ATM Layers:



1. **ATM Adaption Layer (AAL)**

It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

2. **Physical Layer**

It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:

- It converts cells into a bitstream.
- It controls the transmission and receipt of bits in the physical medium.
- It can track the ATM cell boundaries.
- Look for the packaging of cells into the appropriate type of frames.

3. **ATM Layer**

It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

Q9. Explain about various ATM Applications.

Ans:

ATM Applications

1. **ATM WANs**

It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

2. **Multimedia virtual private networks and managed services**

It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.

3. **Frame relay backbone**

Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internet working services.

4. **Residential broadband networks**

ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

5. **Carrier infrastructure for telephone and private line networks**

To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

2.2.4 Exploring Broadband Integrated Services

Q10. Write about broadband integrated services.

Ans: **(Imp.)**

Meaning

The B-ISDN (broadband integrated services digital network) is a virtual circuit-switched network that can use high-speed packet switching services. The B-ISDN will use a flexible multiplexing format called ATM (asynchronous transfer mode).

B-ISDN services are classified into interactive and distribution services. Interactive services contain the bidirectional flow of user information between two subscribers or between a subscriber and a service provider.

Interactive services

The interactive services are further divided into three sub-categories which are as follows-

1. **Conversational**

   Conversational service involves the real-time exchange of information such as sound, video, data or entire documents. Examples include video-telephony, video-conference, and high-speed data transfer. Video-telephony is like the normal video telephony service but also has video capture, transmission and display capabilities. Video-conference supports voice and video communication between two conference rooms or between several individuals.

2. **Messaging**

   Messaging service involves the non-real-time exchange of information between subscribers in a store-and-forward fashion.

3. **Retrieval**

   Retrieval services provide subscribers with retrieval access to centrally-stored public information. Examples include broadband videotext (retrieval of video images/sequences with sound, text and graphics), video retrieval (subscriber create to video libraries of movies) and return of high-resolution pictures and records from multiple archives and data centers.

Distribution Services

Distribution services contain the unidirectional flow of user information from a service provider to a subscriber.

Distribution services are divided into two sub-categories, which are as follows:

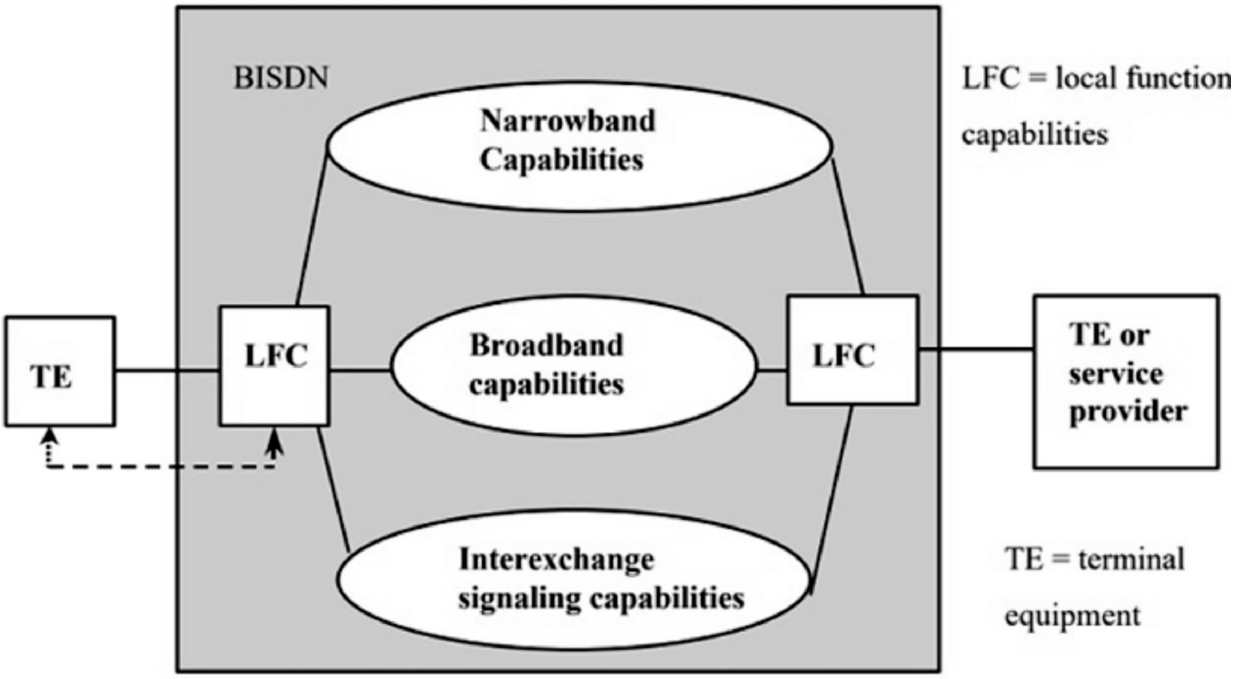
1. Distribution services without user presentation control involve the central broadcast of information to many subscribers, where subscribers have no control over data display. Examples include the broadcast of TV programs, electronic newspapers, and electronic publishing.

2. Distribution services with user presentation control are the same as the previous category. The information is offered as cyclically repeated frames, thereby enabling the subscribers to control the start and the order of the frames presentation. Examples include electronic newspaper and tele-advertising.

Q11. Explain about B-ISDN Architecture.

Ans: **(Imp.)**

The B-ISDN architecture is shown in the diagram below -



The architecture of the B-ISDN includes low Layer capabilities and high Layer capabilities. These capabilities support the services within the B-ISDN and other networks by means of interworking B-ISDN with those networks.

Low Layer capabilities

The low layer capabilities of B-ISDN architecture are explained below -

- From the functional capabilities of the B-ISDN, as shown in Figure, the information transfer capabilities require further description.
- Broadband information transfer is provided by an ATM at the B-ISDN user-network interface (UNI) and at switching entities inside the network.

High Layer capabilities

The high layer capabilities of B-ISDN architecture are explained below -

- Normally, the high Layer functional capabilities are involved only in the terminal equipment.
- The support of some services, provision of high layer functions could be made through special nodes in the B-ISDN belonging to the public network or to centres operated by other organizations and accessed via B-ISDN user-network or network node interfaces (NNIs).

2.2.5 Digital Network Layer And Adaptation Layer

Q12. Explain B-ISDN layers for ATM.

Ans: **(Imp.)**

1) **User plane**

The user plane, with its layered structure, provides for user information flow transfer, along with associated controls (e.g. flow control, and recovery from errors, etc.).

2) **Control plane**

This plane has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections.

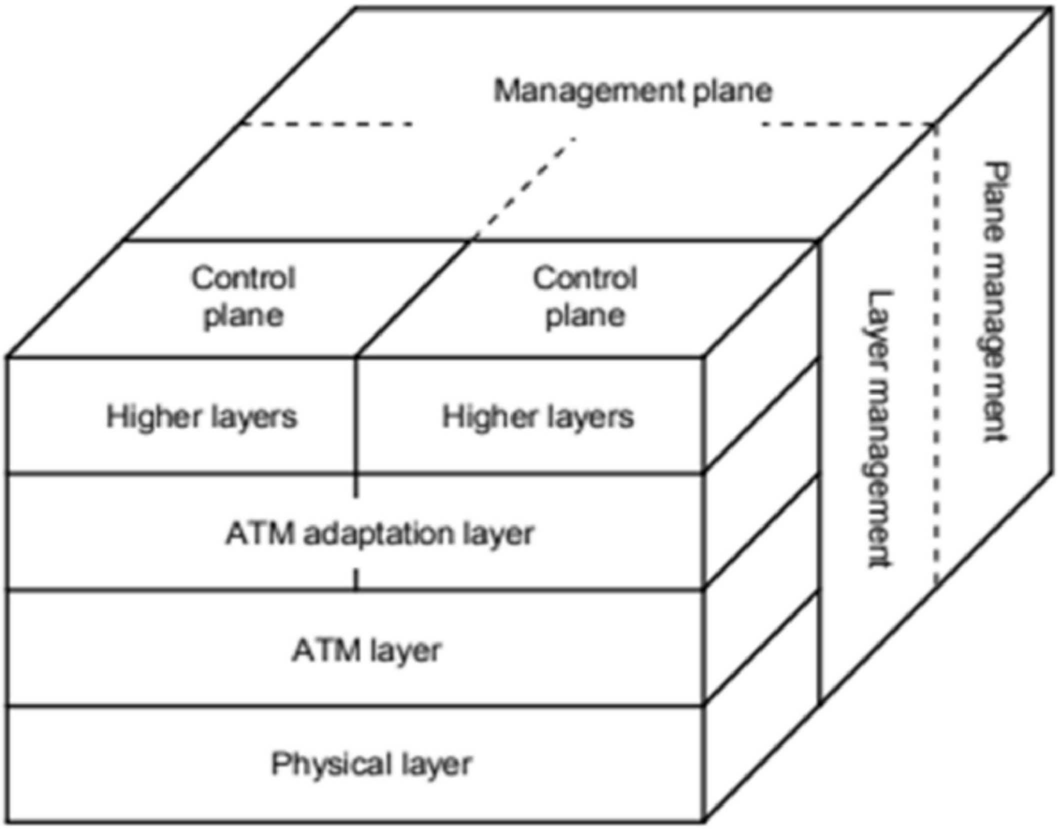
The distinction, if any, between local and global control plane functions in the broadband environment is for further study.

3) **Management plane**

The management plane provides two types of functions, namely Layer Management and plane management functions.

(i) **Plane management functions**

The plane management performs management functions related to a system as a whole and provides coordination between all the planes. Plane management has no layered structure.

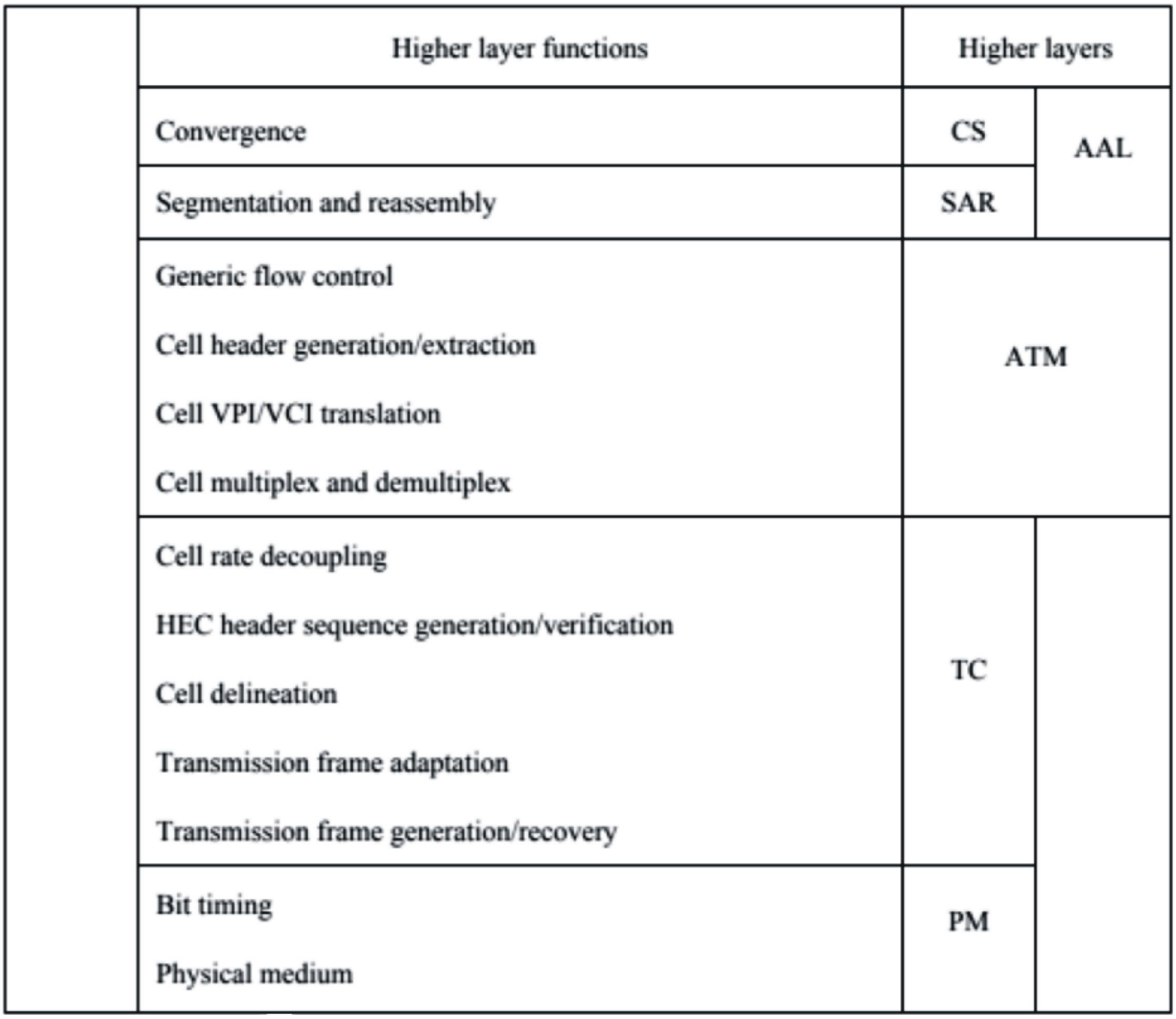


(ii) Layer Management functions

Layer Management performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities. Layer Management handles the operation and maintenance (OAM) information flows specific to the layer concerned.

Functions of the individual layers of the B-ISDN PRM

The functions of each layer, the primitives exchanged between layers, and primitives exchanged between the layers and the management plane are described below. The information flows described do not imply a specific physical realization. Figure illustrates the layers of the PRM, and identifies the functions of the Physical Layer, the ATM Layer, and the AAL.



	Higher layer functions	Higher layers	
	Convergence	CS	AAL
	Segmentation and reassembly	SAR	
	Generic flow control Cell header generation/extraction Cell VPI/VCI translation Cell multiplex and demultiplex	ATM	
	Cell rate decoupling HEC header sequence generation/verification Cell delineation Transmission frame adaptation Transmission frame generation/recovery	TC	
	Bit timing Physical medium	PM	

CS Convergence sublayer
PM Physical medium
SAR Segmentation and reassembly sublayer
TC Transmission convergence

1. Physical layer

The lowest layer in the ATM protocol. It describes the physical transmission media.We can use shielded and shielded twisted pair,Coaxial cable and fibre optic cable.

2. ATM layer

It performs all function relating to the routing and multiplexing of cells over VCs.It generates a header to the segment streams generated bye the AAL, Similarly on the receipt of a cell streams it removes the header from the cell and pass the cell contents to the AAl protocol.To perform all these function, The ATM layer maintains a table which contain a list of VCIs.

3. ATM Adaptation Layer

Top layer in the ATM protocol model. It converts the submitted information into streams of 48-octet segments and transports these in the payload field of multiple ATM cells.Similarly an receipt of the stream of cells relating to the same cell, it converts the 48-octet information field into required form for delivery to the particular higher protocol layer.

Short Question & Answers

1. Explain about circuit switched networks.

Ans :

A network consists of a set of switches that are connected by the physical links commonly known as Circuit-Switched Network.

- Whenever one device communicates with another device then a dedicated communi- cation path is established between them over the network.
- There is only a dedicated channel on each link used by each connection. Also, each link can be easily divided into n channels by using the TDM(Time Division Multiplexing) or FDM(Frequency Divison Multiplexing) technique.
- The Circuit Switching technique is mainly used in the public telephone network for voice communication as well as for data communication.
- Data communication is less efficient than voice communication.

2. Datagram Networks.

Ans:

It is a packet-switching technique in which each packet, known as a datagram, is treated as a separate entity. Each packet carries destination information, which the switch uses to route the packet to the correct destination. There is no need to reserve resources because there is no specified channel for a connection session. As a result, packets contain a header including all of the destination's information. The intermediate nodes examine the header of a packet and choose an appropriate link to a different node closer to the destination.

Resources in datagram networks are allocated on a First Come First Serve (FCFS) basis. When a packet arrives at a router, it must wait if other packets are being processed, regardless of its source or destination.

3. Write Differences between Virtual Circuits & Datagram Networks.

Ans:

S.No.	Basis of comparison	Virtual Circuits	Datagram Networks
1.	Definition	Virtual Circuits are also known as connection-oriented switching. Virtual circuit switching establishes a predetermined path before messages are sent. to the correct destination.	It is a packet-switching technique in which each packet, known as a datagram, is treated as a separate entity. Each packet carries destination information, which the switch uses to route the packet
2.	Connectivity	It is connection-oriented.	It is connectionless.
3.	Path	In these networks, the path taken by the initial data packet between the source and destination nodes is allocated. All subsequent data packets sent between them will take the same path. different paths to their destination.	Since each datagram is treated independently, there is no fixed dedicated path for data transfer. The intermediate routers use dynamically updating routing tables to route each datagram. Therefore, two subsequent packets from the source may travel entirely

4.	Header	Since they are all part of the same virtual circuit, all packets that make up a message have the same header information.	Even though they are part of the same communication, the separate datagram packets have different header information.
5.	Phases	Transmission is performed in three steps: setup, data transfer, and teardown.	There are no such communication phases.
6.	Complexity	In comparison to a datagram network, a virtual circuit is less complex.	However, compared to the virtual circuit, datagram networks are more complex.
7.	Cost	Installation and maintenance costs for virtual circuits are higher.	Networks using datagrams are much easier to set up and maintain.

4. Message Switching.

Ans:

Message Switching is a network switching strategy in which data or message is transmitted entirely from the source to the destination node, one hop at a time. Every intermediary switch in the network stores the entire message during message routing.

If all of the network's resources are used up, or the network becomes blocked, the message-switched network stores and delays the message until sufficient resources are available for effective transmission. Message switching served as an adequate replacement for circuit switching before the development of packet switching. The first applications of it were in data transmissions via telex networks and paper tape relay systems. Although packet switching has completely supplanted message switching, ad hoc sensor networks, military networks, and satellite communications networks still use the technique.

The source node and destination nodes are not directly coupled in message switching. Instead, intermediary nodes (mostly switches) are in charge of transmitting messages from one node to the next. As a result, every intermediary node in the network must retain each message before retransmitting them one at a time as appropriate resources become available. Messages are retained indefinitely if the resources are not available. This process is referred to as store and forward. Every message should include a header, which generally contains routing information such as the source and destination, expiry time, priority level, and so on.

5. ATM.

Ans:

The concept of ATM was developed at first hand itself. In the 1990s, the mobile data carrier speed along with the internet speed saw a boom in the transfer rate. On the other hand, other internet technologies such as voice call and video calls had also started to come into the play. So, in a nutshell, it was not only the internet world but also the telephony world which were converging into each other. Thus networking QoS factors such as latency, jitter, data rate, real-time data delivery, etc., became more important.

It is an International Telecommunication Union - Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

6. Drawbacks of ATM network.

Ans:

Drawbacks

Following are the disadvantages of Asynchronous Transfer Mode (ATM):

- Overhead of cell header (5 bytes per cell)
- Complex mechanisms are used to achieve QoS.
- Congestion may cause cell losses
- ATM switch is very expensive compared to LAN hardware. Moreover ATM NIC is more expensive compared to ethernet NIC.
- As ATM is connection oriented technology, the time required for connection setup and tear down is larger compare to time required to use it.

7. Asynchronous Transfer Mode.

Ans:

Introduction:

ATM stands for Asynchronous Transfer Mode. ATM technology uses ATM cells for data transmission between source and destination. ATM cell uses fixed size of 53 bytes which consists of header (5 bytes) and data (48 bytes). It is behind the success of B-ISDN used for voice/data/video transportation.

ATM transmits cells only when there is data to be transmitted unlike STM (Synchronous Transfer Mode) where bandwidth is assigned periodically like TDM. ATM is connection oriented which uses virtual packet switching. Multiple logical connections are multiplexed over single physical connection.

8. ATM Applications.

1. ATM WANs

It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

2. Multimedia virtual private networks and managed services

It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.

3. Frame relay backbone

Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internet working services.

4. Residential broadband networks

ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

9. Broadband integrated services.

Ans:

The B-ISDN (broadband integrated services digital network) is a virtual circuit-switched network that can use high-speed packet switching services. The B-ISDN will use a flexible multiplexing format called ATM (asynchronous transfer mode).

B-ISDN services are classified into interactive and distribution services. Interactive services contain the bidirectional flow of user information between two subscribers or between a subscriber and a service provider.

10. Functions of the individual layers of the B-ISDN PRM.

Ans:

1. Physical layer

The lowest layer in the ATM protocol. It describes the physical transmission media.We can use shielded and shielded twisted pair,Coaxial cable and fibre optic cable.

2. ATM layer

It performs all function relating to the routing and multiplexing of cells over VCs.It generates a header to the segment streams generated bye the AAL, Similarly on the receipt of a cell streams it removes the header from the cell and pass the cell contents to the AAI protocol.To perform all these function, The ATM layer maintains a table which contain a list of VCIs.

3. ATM Adaptation Layer

Top layer in the ATM protocol model. It converts the submitted information into streams of 48-octet segments and transports these in the payload field of multiple ATM cells.Similarly an receipt of the stream of cells relating to the same cell, it converts the 48-octet information field into required form for delivery to the particular higher protocol layer.

Choose the Correct Answers

1. A _______ network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both. [a]

   (a) Virtual-circuit (b) Packet-switched

   (c) Frame-switched (d) None of the above

2. Circuit switching can involve the use of _______. [d]

   (a) Space division switches (b) Time domain switches

   (c) TDM bus (d) All of the above

3. There are two popular approaches to packet switching : [d]

   (a) Datagram (b) Virtual circuit

   (c) TDS (d) Both option A & B

4. Datagram networks mainly refers to _______. [b]

   (a) Connection oriented networks (b) Connection less networks

   (c) Telephone networks (d) Internetwork

5. Packets in datagram switching are referred to as _______ [c]

   (a) Switches (b) Segments

   (c) Datagrams (d) Data-packets

6. Which of the following is not a phase of virtual circuit network? [c]

   (a) Setup phase (b) Data transfer phase

   (c) Termination phase (d) Teardown phase

7. In virtual circuit network, the number of delay times for setup and teardown respectively are _______ [a]

   (a) 1 and 1 (b) 1 and 2

   (c) 2 and 1 (d) 2 and 2

8. Store and forward are terms used to describe _______ switching. [c]

   (a) Circuit (b) Packet

   (c) Message (d) All of the above

9. Each ATM _______ contains a table to identify paths to other switches [b]

   (a) Cell (b) Switch

   (c) Station (d) a and b

10. An ATM cell consists of _______ bytes. [b]

   (a) 48 (b) 53

   (c) 256 (D) a variable number of

Fill in the blanks

1. The required resources for communication between end systems are reserved for the duration of the session between end systems in _______ method.
2. Store and forward are terms used to describe _______
3. In a _______ network , data are transmitted in discrete units of potentially variable length blocks called packets.
4. A _______ network is a cross between a circuit-switched network and a datagram network.
5. In a packet-switching technique in which each packet, known as a _______
6. During teardown phase, the source, after sending all the frames to destination, sends a _______ to notify termination.
7. The simplest ATM switch is the _______ switch.
8. The _______ layer accepts transmissions from upper-layer services.
9. The _______ is a virtual circuit-switched network that can use high-speed packet switching services.
10. B-ISDN services are classified into_______ and _______services

Answers

1. Circuit switching
2. Message Switching
3. Packet switching
4. Virtual-circuit
5. Datagram
6. Teardown request
7. Crossbar
8. AAL
9. B-ISDN (broadband integrated services digital network)
10. Interactive and distribution

UNIT III

IPv4 :

Address Space, Notations, Classful, Classless, Network Address Translation, Datagram, Fragmentation and Checksum IPv6 Addresses: Structure, Address Space, Packet Format and Extension Headers, ICMP, IGMP, ARP, RARP, Congestion Control and Resource Allocation: Problem, Issues, Queuing, TCP

3.1 IPv4 Address Space

Q1. What is address space? Explain about it.

Ans : **(Imp.)**

Address space is the amount of memory allocated for all possible addresses for a computational entity for example, a device, a file, a server or a networked computer. The system provides each device and process address space that holds a specific portion of the processor's address space. This can include either physical or virtual addresses accessible to a processor or reserved for a particular process.

The width of its address bus and registers often restricts the processor's address space. However, a memory management technique called virtual memory can increase the size of the address space to be higher than that of the physical memory.

Address space is classified as either flat or segmented. Flat address spaces are represented by incrementally increasing integers starting at zero. Independent segments augmented by offsets or values added to create secondary addresses represent segmented addresses.

In some systems, address space can be converted from one format to another through a thinking process — low-level, machine-generated code used to deploy details of a software system. Thanking is often used to delay calculations until the system requires a result.

Some types of address spaces

Here are a few examples of address spaces.

1. Virtual address space

A binary number in the virtual memory that allows processes to use a location in primary storage is a virtual address. This accommodates use of the main memory, independent of other processes, and supports the use of more space than what actually exists. It works by relegating some content to a hard disk or internal flash drive.

2. Logical address space

A logical address space is a set of logical addresses a computer generates for a specific program. A group of physical addresses mapped to corresponding logical addresses is called a physical address space.

3. IPv4 to IPv6

In terms of IP address space, concern emerged that the 32-bit address space of IP version 4 (IPv4) would be inadequate to support the enormous growth of the internet. So, IPv6 was developed with its 128-bit address space.

4. Subnetting IPv6 address space

The primary purpose of subnetting IPv6 address space is to improve address allocation efficiency by subnetting a segment of a network address space. Splitting an extensive network into smaller groups of interconnected networks reduces traffic, which helps increase network speeds because traffic does not have to flow through unnecessary routes. The subnet mask shares the network portion of the IP address and the host address range with the computer. The host address range comprises addresses assigned to host computers on the network.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

3.1.1 Notations

Q2. Explain about notations used in IPv4 and IPv6.

Ans : **(Imp.)**

Dotted Decimal Notation

We have seen that the IPv4 address is expressed as a 32-bit number in dotted decimal notation. IP addresses may have a fixed part and variable part depending upon the allocation of total addresses to you or your organization.

The fixed part of the address may be from one octet to three octets, and the remaining octets will then be available for the variable part.

For example, you can take an IP address like 192.168.10.25. Now set all constant bits to 1 and set all variable bits to 0. This gives 11111111 11111111 00000000 On converting it in dotted-decimal notation, the outcome is 255.255.0.0.

This dotted-decimal notation with constant and variable methods can address prefixes to 192.168.10.25 and is represented as 192.168.10. 25, 255.255.0.0. This method of expressing the prefix length as a dotted-decimal number is known as a network mask or subnet mask notation.

Slash Notation

It is also known as CIDR (Classless Inter-Domain Routing) notation.

IPv4

Slash notation is a compact way to show or write an IPv4 subnet mask. When you use slash notation, you write the IP address, a forward slash (/), and the subnet mask number.

To find the subnet mask number:

1. Convert the decimal representation of the subnet mask to a binary representation.
2. Count each “1” in the subnet mask. The total is the subnet mask number.

For example, to write the IPv4 address 192.168.42. 23 with a subnet mask of 255.255.255.0 in slash notation:

1. **Convert the subnet mask to binary**

   In this example, the binary representation of 255.255.255.0 is:

   11111111.11111111.11111111.00000000.

2. **Count each 1 in the subnet mask**

   In this example, there are twenty-four (24).

3. **Write the original IP address, a forward slash (/), and then the number from Step 2.**

   The result is 192.168.42.23/24.

This table shows common network masks and their equivalents in slash notation.

Network Mask	Slash Equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

IPv6

In IPv6, slash notation is used to represent the network identifier prefix for an IPv6 network. The prefix is expressed as a slash (/) followed by the prefix size, which is a decimal number between 1 and 128. The CIDR notation works exactly the same as with IPv4, which means if you have a /48, that means the first 48 bits of the address are the prefix.

This table shows common IPv6 network prefixes and the number of IPv6 subnets and IPv6 addresses they support.

Prefix	Number of Subnets
/64	1 IPv6 subnet with up to 18,446,744, 073,709,551,616 IPv6 host addresses
/56	256 /64 subnets
/48	65,536 /64 subnets

A network site that is assigned a /48 prefix can use prefixes in the range /49 to /64 to define valid subnets.

3.1.2 CLASS FULL

Q3. What is class full addressing? Explain

Ans :

Classfull Addressing

The 32 bit IP address is divided into five sub-classes. These are:

1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

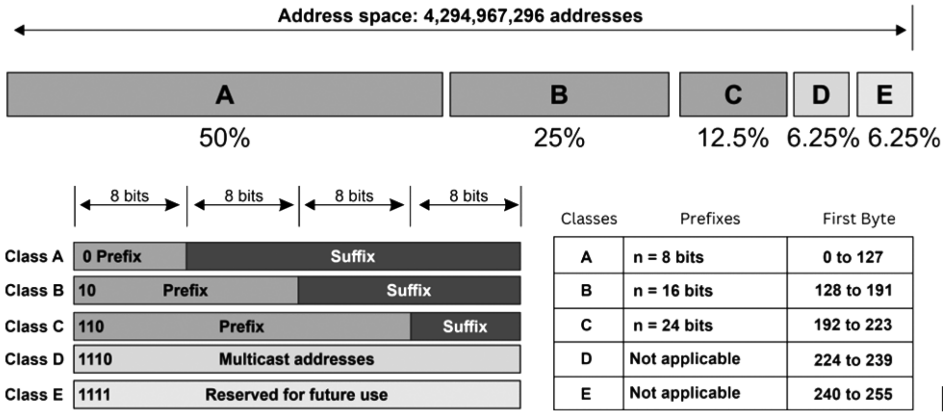
Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.

Occupation of the address space in classful addressing



Classes	Prefixes	First Byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

1. CLASS A

Despite the fact that the network length is 8 bits, we can only use seven bits for the network identifier since the first bit, which is 0 and determines the class, is part of the length. This indicates that only $2^7 = 128$ networks can have a class A address globally.

- Net ID = 8bits long and Host ID = 24 bits long
- Method to identify class A addresses:
  - The first bit is reserved to 0 in binary
  - Range of the first octet is [0, 127] in dotted decimal
- Total number of connections in Class A = 2^{31} (2, 14, 74, 83, 648)
- There are $2^7 - 2 = 126$ networks in the Class A network.
  - There are 2 fewer networks available overall since IP Address 0.0.0.0 is set aside for broadcasting needs. For usage as a loopback address while testing software, the IP address 127.0.0.1 is set aside.
  - Hence, the range of the first octet becomes [1, 126]
- Total number of Host IDs in Class A = 2^{24} - 2 [1, 67, 77, 214]
  - There are 2 fewer hosts that can be established across all classes due to the two reserved IP addresses, where all of the host ID bits are either zero or one.
- The Network ID for the network is represented when all of the Host ID bits are set to 0.
- The Broadcast Address is represented when all of the Host ID bits are set to 1.
- Organizations needing very large networks, like Indian Railways, employ class A.

2. CLASS B

Despite the fact that the first two bits of class B's network, which are 10 in binary or we can write it as $(10)_2$, determine the class, we can only use 14 bits as the network identification, as class B's network length is 16 bits. As a result, only $2^{14} = 16{,}384$ networks in the entire world are capable of using a class B address.

- Length of Net Id = 16 bits and length of Host ID 16 bits.
- Method to identify Class B networks:
- First two bits are reserved to 10 in binary notation
- The Range of the first octet is [128, 191] in dotted decimal notation
- Total number of connections in the class B network is $2^{30} = 1, 07, 37, 41, 824$
- Total number of networks available in class B is $2^{14} = 16, 384$
- Total number of hosts that can be configured in Class B = 2^{16} - 2 = 165, 534
- Organizations needing medium-sized networks typically utilize class B.

3. CLASS C

All addresses that begin with the number $(110)_2$ fall under class C. Class C networks are 24 bits long, but since the class is defined by three bits, the network identifier can only be 21 bits long. As a result, $2^{21} = 2, 097, 152$ networks worldwide are capable of using a class C address.

- The length of the Net Id and the Host Id = 24 bits and 16 bits respectively.
- Method to identify Class C networks:

- First three bits are reserved for 110 in binary notation or $(110)_2$.
- The range of the first octet is [192, 223] in dotted decimal notation.
- Total number of connections in Class C = $2^{29} = 53, 68, 70, 912$.
- Total number of networks available in Class C = $2^{24} = 20, 97, 152$.
- Total number of hosts that can be configured in every network in Class C = $2^8 - 2 = 254$.
- Organizations needing small to medium-sized networks typically choose class C.

4. CLASS D

Prefix and suffix categories do not exist for Class D. It is employed for multicast addresses.

- There is no concept of Host ID and Net ID
- Method to identify Class D network:
- The first four bits are reserved to 1110 in binary notation or $(1110)_2$
- The range of the first octet is [224, 239] in dotted decimal notation
- Total number of IP addresses available is $2^{28} = 26, 84, 35, 456$
- Because data is not intended for a specific host, Class D is set aside for multicasting, which eliminates the requirement to extract the host address from the IP address.

5. CLASS E

All binary addresses with the prefix 1111 fall under class E. Class E, like Class D, does not have a prefix or a suffix and is used as a reserve.

- Like in Class D, there is also no concept of Host ID and Net ID.
- Method to identify Class E networks:
- The first four bits are reserved to 1111 in binary notation or (1111)
- The range of the first octet is [240, 255] in dotted decimal notation.
- Total number of IP addresses available is $2^{28} = 26{,}84{,}35{,}456$.
- Class E is set aside for hypothetical or experimental uses.

Rules for assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

3.1.3 CLASSLESS

Q4. Write about classless addressing.

Ans :

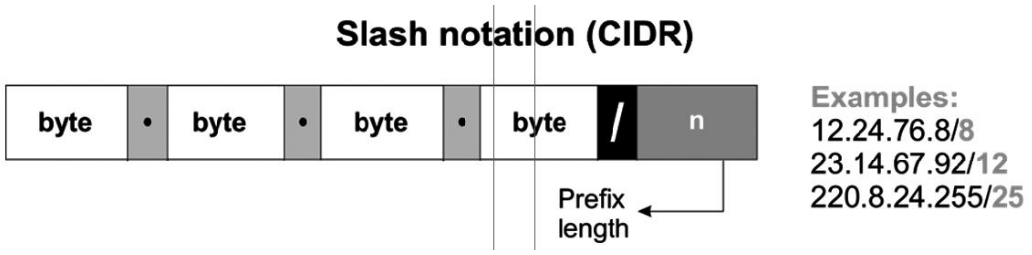
The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses. In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22 ,..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses. In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22 ,..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.

In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n. Slash notation is the colloquial name for the notation, while classless interdomain routing, or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.



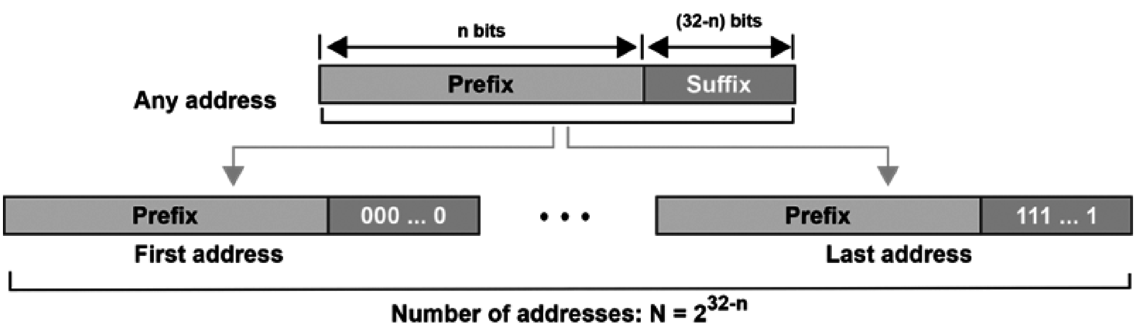
To put it another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

Extracting Information from an Address

With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n, is known.

- The block has N = 232n addresses, according to the calculation.
- The n leftmost bits are kept, and the (32 - n) rightmost bits are all set to zeroes to determine the first address.
- The n leftmost bits are kept, while the (32 - n) rightmost bits are all set to 1s to determine the last address.

Information extraction in classless addressing



For Example

The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are $2^{32-n} = 2^5 = 32$ addresses in all.

The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.

Address: 167.199.170.82/27 10100111 11000111

10101010 01010010

Last address: 167.199.170.64/27 10100111 11000111

10101010 01000000

Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.

Address: 167.199.170.82/27 10100111 11000111

1010101001011111

Last address: 167.199.170.95/27 10100111 11000111

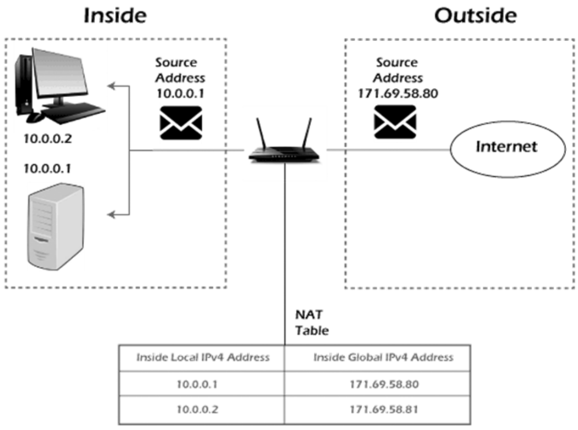
1010101001011111

3.1.4 Network Address Translation

Q5. What is Network Address Translation? Explain

Ans : **(Imp.)**

NAT (Network Address Translation) connects two networks and maps the private (inside local) addresses into public addresses (inside global). Inside local denotes that the best address belonged to an internal network and was not assigned by a Network Information Centre or service power. The inside global signifies that the address is a valid address assigned by the NIC or service provider, and one or more inside local addresses to the outside world.



Inside Local IPv4 Address	Inside Global IPv4 Address
10.0.0.1	171.69.58.80
10.0.0.2	171.69.58.81

NAT is a method of converting a private IP address or a local address into a public IP address. NAT is a technique for reducing the rate at which available IP addresses are depleted by translating a local IP or private IP address into a global or public IP address. The NAT relation might be one-to-one or many-to-one.

Furthermore, NAT can only configure one address in order to represent the entire network to the outside world. As a result, the translation process is transparent. NAT can be used to migrate and merge networks, share server loads, and create virtual servers, etc.

Types of NAT

There are three types of NAT:

1. Static NAT

In static NAT, a local address is mapped to a global address. In this type of NAT, the relationship is one-to-one. Static NAT is used if a host needs a consistent address that must be acceded from the internet. For example, networking devices or enterprise servers.

2. Dynamic NAT

Unregistered private IP addresses can be converted to registered public IP numbers from a pool of public IP addresses using dynamic NAT.

3. PAT/NAT Overloading/IP masquerading

Among the three varieties, PAT is the most famous. It's a form of Dynamic NAT that's comparable to it, but it uses ports to translate many private IP addresses to a single public IP address.

4. Network Address Translation (NAT) working

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

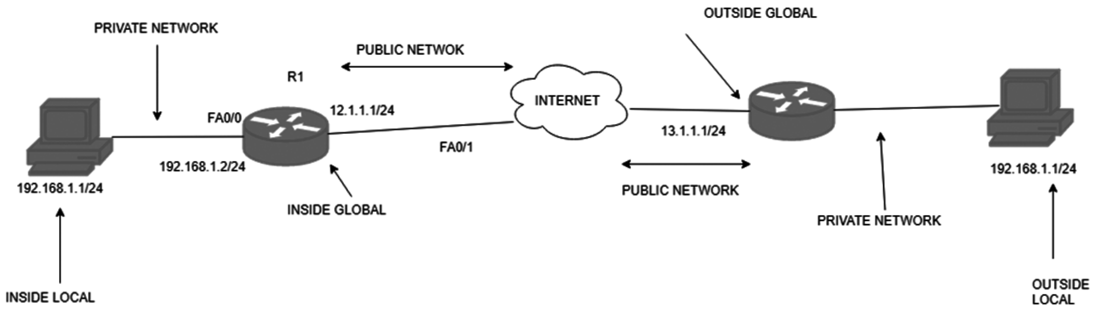
➢ If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Mask port numbers

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address:** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address:** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address:** This is the actual IP address of the destination host in the local network after translation.
- **Outside global address:** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types

There are 3 ways to configure NAT:

1. **Static NAT:** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

   Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT:** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

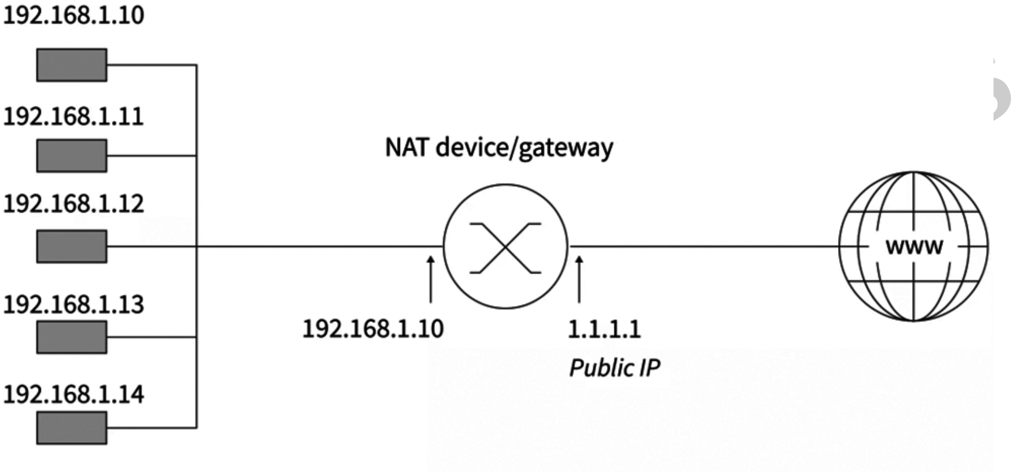
   Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT):** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

NAT(Network Address Translation) Examples

When a host on the internal or private network with an internal IP address needs to communicate with a device outside of the private network, it will use the public IP address on the network's gateway to identify itself to the outside world, and NAT would translate the private IP address into the public address. If, for instance, a computer with the internal address 192.168.1.10 192.168.1.10 wished to communicate with a web server on the internet, NAT would translate that address to the company's public address, which we'll name in this case 1.1.1.11.1.1.1.

So that when communicating with the outside world, the internal address is recognized as the public address. This is necessary because, for the webserver to respond to this internal computer, it would need to transmit the response to the public address, which is a distinct and routable address on the internet. The private address is secret, non-routable, and concealed from the outside world, the original address of 192.168.1.10192.168.1.10 cannot be used. The public address for that company would be this one at 1.1.1.11.1.1.1, which is visible to everyone.



Network Address Translation

The web server would now respond to that 1.1.1.11.1.1.1 public address. NAT would use its records to convert the packets received from the web server intended for 1.1.1.11.1.1.1 back to the internal network address of 192.168.1.10192.168.1.10 so that the computer that requested the original information would get the requested packets.

The two advantages of NAT are now readily apparent. First, it would reduce the number of IP addresses we need because not every computer needs a public address. Second, it would shield these private computers from prying eyes. Only the public address is visible to everyone, everything else is concealed behind it. Therefore, nothing past the public address on the firewall's or router's external interface may be seen from the internet.

Advantages of NAT

The following are the advantages of NAT:

- NAT protects the public addresses that have been registered and slow down the IP address space exhaustion.
- Removes the address renumbering process that occurs when switching networks
- The occurrence of address overlap was significantly reduced.
- Increases flexibility of the connection establishment.

Disadvantages of NAT

The following are the disadvantages of NAT:

- Lack of end-to-end traceability
- Certain applications are not compatible with NAT
- Switching path delays are the outcome of the translation

3.1.5 DATAGRAM

Q6. Explain about datagram network

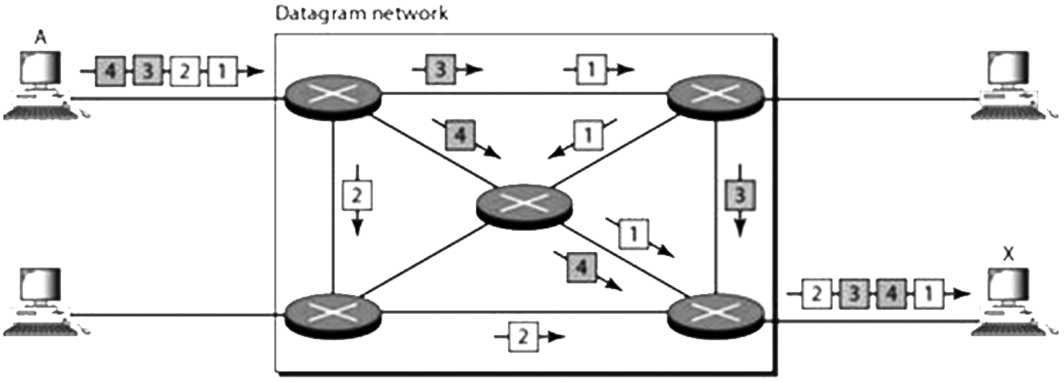
Ans : **(Imp.)**

In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.

In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first come, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed.

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multi packet transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.

The following figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.



In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application. The datagram networks are sometimes referred to as connectionless networks.

Routing Table

In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.

Destination Address

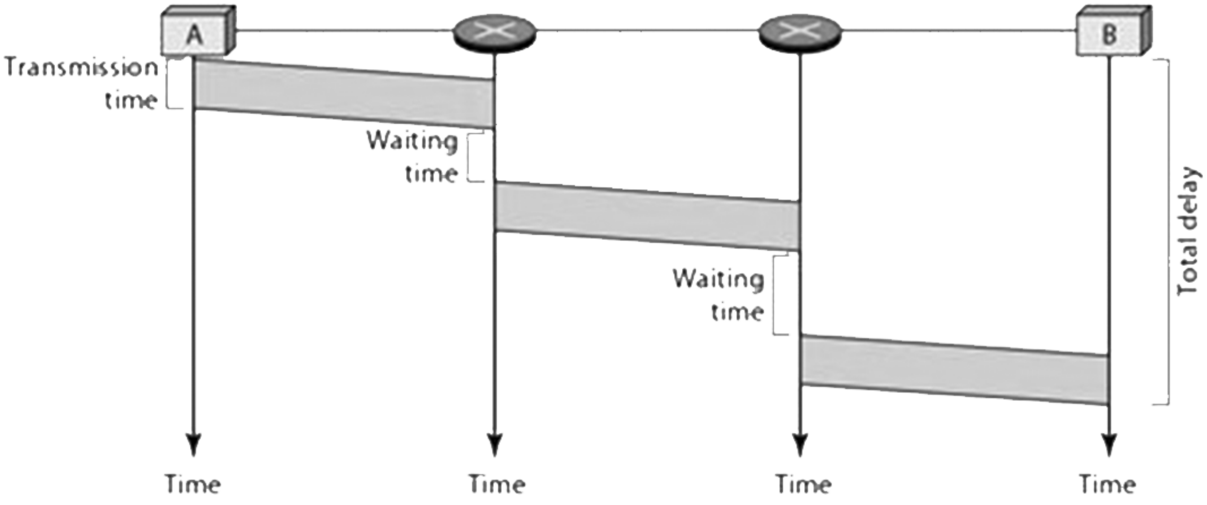
Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network. Resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message. The following figure gives an example of delay in a datagram network for one single packet.



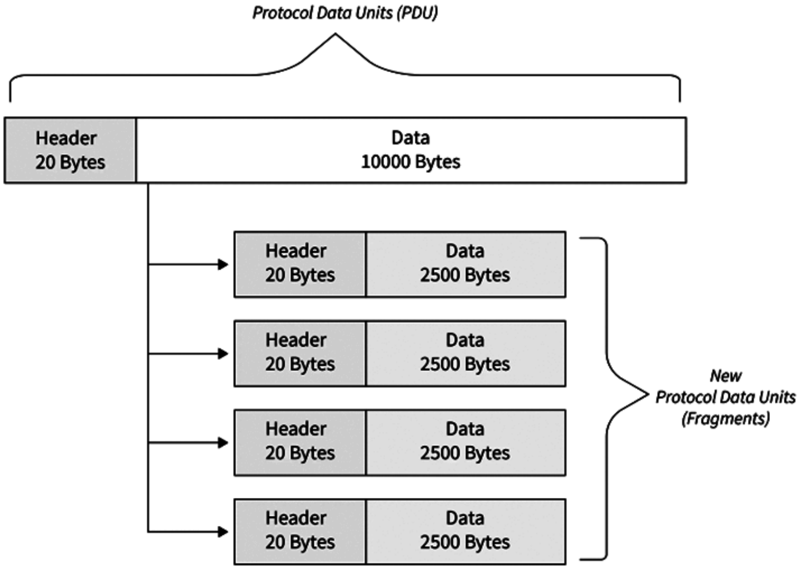
The Internet has chosen the datagram approach to switching at the network layer. It uses the universal addresses defined in the network layer to route packets from the source to the destination.

3.1.6 Fragmentation and Checksum

Q7. What is Fragmentation in Networking? Explain.

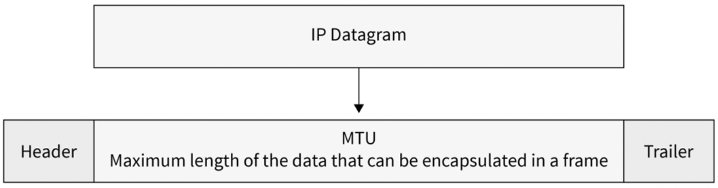
Ans : **(Imp.)**

IP fragmentation is a process that divides packets into smaller pieces (fragments) so that the resulting pieces can travel across a link with a smaller maximum transmission unit (MTU) than the original packet size. The receiving host reassembles the fragments.



An IP packet cannot be larger than the maximum size allowed by that local network when sent over the network by a host. The network's data link and IP Maximum Transmission Units (MTUs), which are typically the same, determine its size. 1500 byte MTUs are standard for modern Ethernet-based office, campus, or data center networks.

However, packets initially delivered across a network with one MTU may need to be routed over networks with a smaller MTU (such as a WAN or VPN tunnel). If the packet size in these circumstances is greater than the lower MTU, the data in the packet must be fragmented (if possible). This indicates that it is divided into fragments carried in brand-new packets (fragments) that are equal to or less than the lower MTU. This is known as fragmentation, and when the fragments arrive at their destination, the data is usually put back together.


IP Datagram
Header
MTU
Maximum length of the data that can be encapsulated in a frame
Trailer

Frame

Some points related to the fragmentation:

- The maximum size of an IP datagram is 216"1=65,535216"1=65,535 bytes, as the IP header has a total length of 16 bits.
- It is performed by the network layer at the destination side, typically at routers.
- Due to intelligent (*excellent*) segmentation by the transport layer, the source side does not require fragmentation. Specifically, the transport layer looks at the datagram and frame data limits and segments the data so that it can easily fit in a frame without the need for fragmentation.
- The receiver uses the identification (16 bits) field in the IP header to identify the packet. The identification number for each frame fragment is the same.
- The receiver uses the fragment offset(13 bits) field in the IP header to identify the series of frames.

- The extra header created by fragmentation results in overhead at the network layer.

Process of Fragmentation

RFC 791 specifies IP packet fragmentation, transmission, and reassembly mechanism.

RFC 815 specifies a streamlined reassembly algorithm. The Identification field in the IP header, along with the foreign and local internet addresses and the protocol ID, and the Fragment offset field in the IP header, coupled with the Don't Fragment and More Fragments flags, are used for fragmentation and reassembly of IP packets.

If a receiving host receives a fragmented IP packet, it must put the packet back together and send it to the higher protocol layer. Reassembling is supposed to occur in the receiving host, but in reality, it might be carried out by an intermediate router. For instance, *network address translation (NAT)* can need to reassemble fragments to translate data streams.

Fields in IP Header for Fragmentation

Fields in IP header for fragmentation

- **Identification (16 bits):** use to identify fragments of the same frame.
- **Fragment offset (13 bits):** use to identify the sequence of fragments in the frame. It generally indicates a number of data bytes preceding or ahead of the fragment.

Maximum fragment offset possible = (65535 – 20) = 65515 {where 65535 is the maximum size of datagram and 20 is the minimum size of IP header}

So, we need ceil($\log_2$65515) = 16 bits for a fragment offset but the fragment offset field has only 13 bits. So, to represent efficiently we need to scale down the fragment offset field by $2^{16}/2^{13}$ = 8 which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset " N.

- **More fragments (MF = 1 bit): –** tells if more fragments are ahead of this fragment i.e. if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.
- **Don't fragment (DF = 1 bit) –** if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

IP Fragmentation Examples

Now let's understand the concept of IP fragmentation with the help of an example.

- In network X, a host named A has an MTU of 520 bytes.
- In network Y, a host named B has an MTU of 200 bytes.
- Host A of network X wants to send a message to host B in network Y.

Assume a router gets a datagram from host A that contains:

- The length of the header is 20 bytes.
- The length of the payload is 500 bytes.
- The whole length is 520 bytes.
- The *DF* bit is set to 0. The router now operates in the following steps:

Step 1

The router looks through the datagram and discovers:

- The datagram has a size of 520 bytes.
- Network Y is the destination, and its MTU is 200 bytes.
- The DF bit is set to 0.

The router concludes:

- The datagram's size exceeds the *MTU*.
- It must therefore break the datagram into fragments.
- *DF* bit has been set to 0.
- Therefore, it is acceptable to create datagram fragments.

Step 2

The router determines the amount of data that should be transmitted in each fragment.

The router is aware of:

- The destination network's MTU is 200 bytes.
- Therefore, any fragment can only have a maximum total length of 200 bytes.

- The header will take up 20 bytes out of the total 200 bytes.
- Thus, 180 bytes is the maximum amount of data that can be delivered in any fragment.

The router uses the following rule to determine how much data will be delivered in a single fragment:

Rule

The quantity of data delivered in a single fragment is chosen in such a way that-

1. It is as large as feasible but less than or equal to *MTU*.
2. It is a multiple of 8, so a pure decimal value for the fragment offset field can be obtained.
   - The final fragment is not required to contain data in multiples of 8, though.
   - This is because it need not determine the fragment offset value for any other fragment.

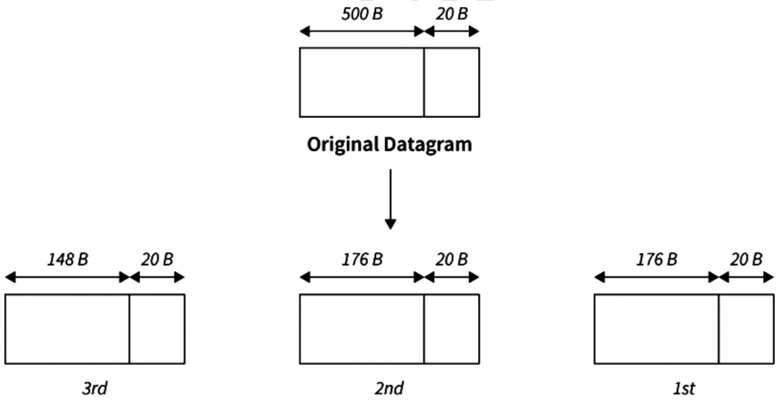
Following the above rule,

- The router determines a maximum of 176 bytes of data that can be sent in one fragment.
- This is because it is the highest figure that is less than *MTU* and a multiple of 8.

Step 3

The router splits the original datagram into three parts where:

- The first fragment contains data = 176 bytes.
- The second segment has data = 176 bytes.
- The third fragment contains data = 148 bytes.



Fragments of Original Datagram

Each fragment's IP header contains information:

Header information of 1st fragment

- Field value for header length = 20/4=520/4=5.
- Total length field value = 176+20=196176+20=196.
- MF bit = 1.
- The value of the fragment offset field is 0.
- The header checksum is updated.
- The identification number is the same as the original datagram.

Header information of 2nd fragment

- Field value for header length = 20/4=520/4=5.
- Total length field value = 176+20 =196176 + 20 = 196.
- MF bit = 1.
- The value of the fragment offset field is 176/8=22176/8=22.
- The header checksum is updated.
- The identification number is the same as the original datagram.

Header information of 3rd fragment

- Field value for header length = 20/4=520/4=5.
- Total length field value = 148+20 = 168148 + 20=168.
- MF bit = 0.
- The value of the fragment offset field is (176+176)/8=44(176+176)/8=44.
- The header checksum is updated.
- The identification number is the same as the original datagram.

The router retransmits all the fragments.

Step 4

On the destination side,

- The receiver receives three datagram fragments.
- To get the original datagram, the reassembly algorithm is used to combine all of the fragments.

Q8. Why is Fragmentation Needed?

Ans :

The datagram generated by the network layer at the source computer must traverse many networks before arriving at the destination computer. Typically, the source computer favors sending large datagrams. This is because if the datagram is broken up into smaller pieces, the header will be repeated for each datagram unit. The header is repeated for every fragmented datagram, wasting network bandwidth.

However, each network has a cap on the largest packet size it can send during this occurrence. Even worse, the source computer is unaware of the packet's route to get to its destination. It cannot, therefore, determine how small each fragmented datagram must be. The reasons for fragmenting a large datagram into a small fragmented datagram are listed below:

1. The capacity of data is limited by the hardware and operating system employed.
2. Conformity with national and international norms.
3. Each network's protocols allow for different packet sizes.
4. Large packets occupy the network for a longer time than small packets.
5. Reduce the mistake caused by retransmission.

Q9. What is Checksum? How to apply checksum for error detection? Explain.

Ans : **(Imp.)**

The checksum is a network method to check for any error or damage to the data transmitted to the sender side from the sender side. The checksum method applies the bit addition and bit complement method to perform the checksum implementation.

The need to apply checksum or any other error-detection method is done simply to identify the damage to the data when it's being transmitted over the network channel.

The checksum uses the Checksum Generator on the sender side and the Checksum Checker on the receiver side.

Working Steps for Checksum

Steps involved in the checksum error-detection method:

Step 1: At the Sender Side

- Divide the original data into the 'm' number of blocks with 'n' data bits in each block.
- Adding all the 'k' data blocks.
- The addition result is complemented using 1's complement.
- The obtained data is known as the Checksum.

Step 2: Data Transmission

- Integrate the checksum value to the original data bit.
- Begin the transmission of data to the receiver side.

Step 3: At the Receiver Side

- Divide the received data into the ‘k’ number of blocks.
- Adding all the ‘k’ data blocks along with the checksum value.
- The addition result is complemented using 1’s complement.
- Two possible cases after 1’s complement:
- Case 1: If the result is 0.
- No errors in the received data from the sender side.
- The receiver accepts the data.
- Case 2: If the result is not 0.
- Errors in the received data from the sender side.
- The receiver discards the data and requests for retransmission of data.

Solved Example

Let’s use an example to implement the checksum method and consolidate our understanding of the network principle.

For the given data value 11001100 10101010 11110000 11000011, perform the checksum method.

1. The first step is to perform the bit addition of the given data bits at the sender side.

```
Sender Side:
                1   0   0   1   1   0   0   1
                1   1   1   0   0   0   1   0
                0   0   1   0   0   1   0   0
                1   0   0   0   0   1   0   0
              ________________________________
                0   0   1   0   0   0   1   1
                                        1   0
              ________________________________
                0   0   1   0   0   1   0   1
```

Note: The extra carry bits are added to the summation result.

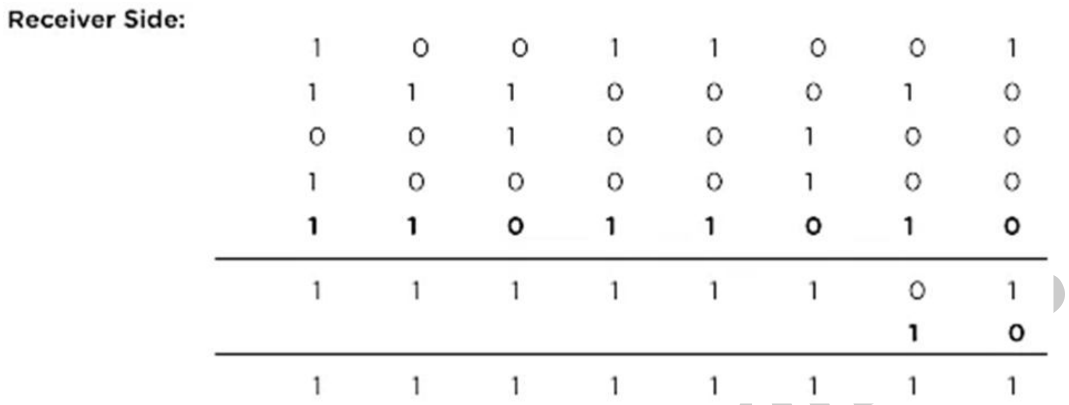
2. Perform the 1’s Complement for the bit addition result, thus obtaining the checksum value.

```
Sender Side:
          0   0   1   0   0   1   0   1
                 1’s Complement
                       ⬇
Checksum
          0   0   1   0   0   1   0   1
```

3. Integrate the checksum value and the original data bit and begin the data transmission to the receiver.

11011010	10011001	11100010	00100100	10000100

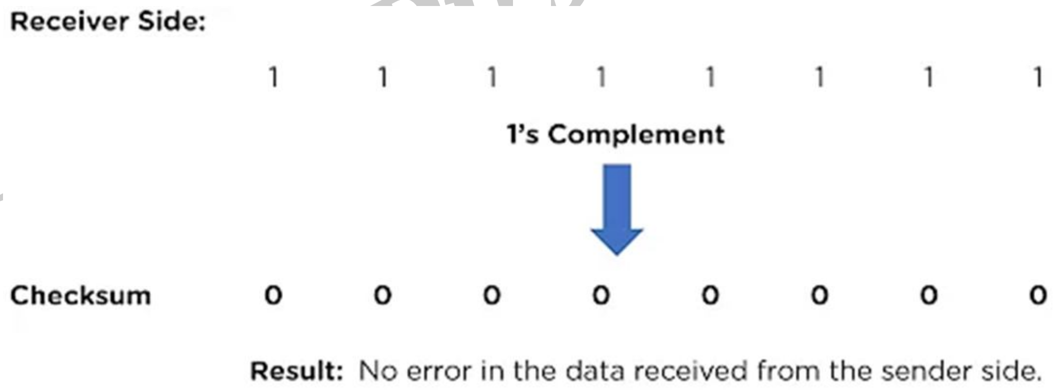
4. The receiver side will begin the Checksum Checker method, repeat the bit addition, and perform the 1's complement.



Receiver Side:

```
1   0   0   1   1   0   0   1
1   1   1   0   0   0   1   0
0   0   1   0   0   1   0   0
1   0   0   0   0   1   0   0
1   1   0   1   1   0   1   0
-----------------------------
1   1   1   1   1   1   0   1
                        1   0
-----------------------------
1   1   1   1   1   1   1   1
```

5. If the complement result is 0, the data received is correct and without any error.



Receiver Side:

```
1   1   1   1   1   1   1   1
```

1's Complement

```
Checksum   0   0   0   0   0   0   0   0
```

Result: No error in the data received from the sender side.

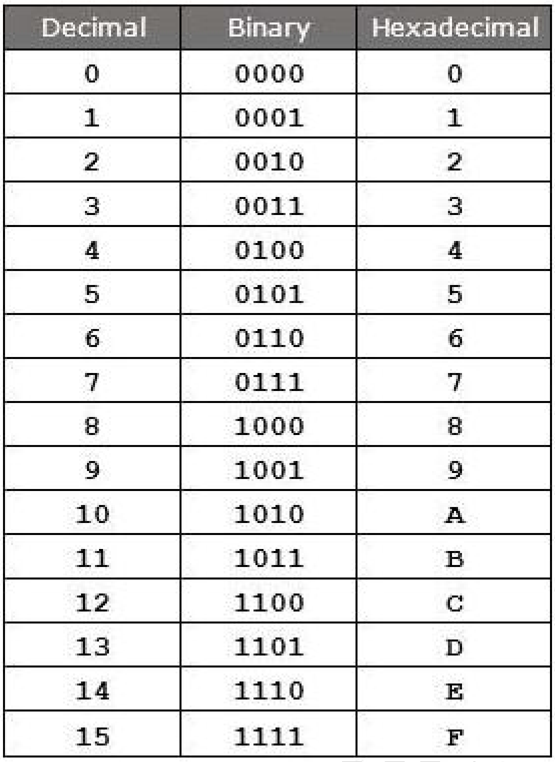
3.2 IPV6 Addresses

3.2.1 Structure

Q10. Explain the structure of IPV6

Ans : **(Imp.)**

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is a positional number system that uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.



Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001

0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero(es)

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2:

If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

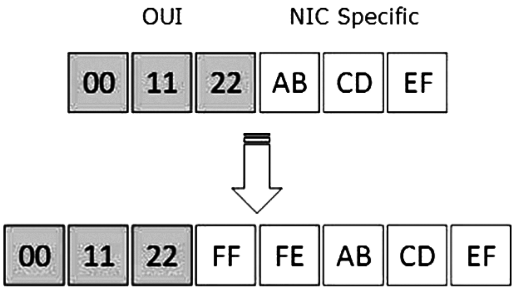
2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

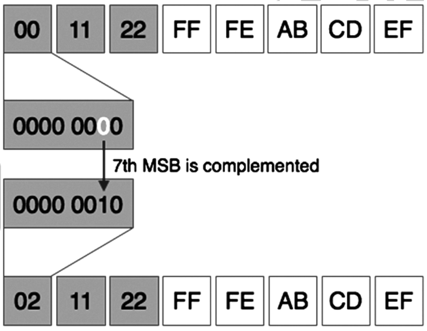
Interface ID

IPv6 has three different types of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. The MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC addresses are considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses. A host can auto-configure its Interface ID by using IEEE's Extended Unique Identifier (EUI-64) format. First, a host divides its own MAC address into two 24-bits halves. Then 16-bit Hex value 0xFFFE is sandwiched into those two halves of MAC address, resulting in EUI-64 Interface ID.



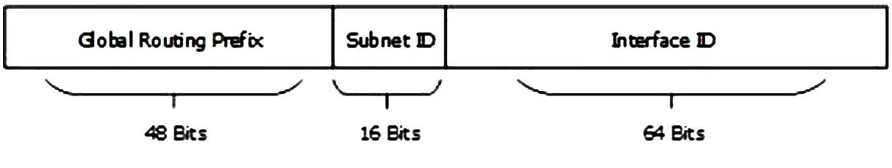
Conversion of EUI-64 ID into IPv6 Interface Identifier

To convert EUI-64 ID into IPv6 Interface Identifier, the most significant 7th bit of EUI-64 ID is complemented. For example:



Global Unicast Address

This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

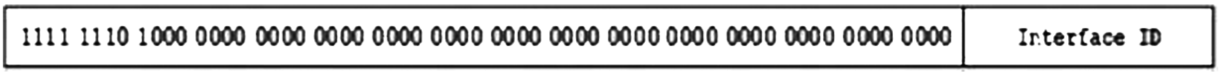


Global Routing Prefix

The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific autonomous system. The three most significant bits of Global Routing Prefix is always set to 001.

Link-Local Address

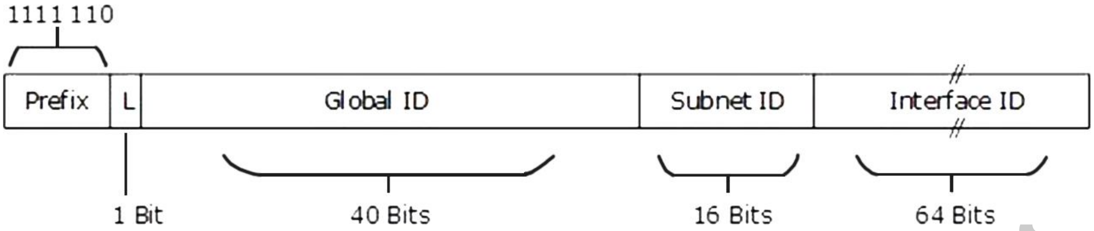
Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0, thus:



Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable, so a Router never forwards these addresses outside the link.

Unique-Local Address

This type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



Prefix is always set to 1111 110. L bit, is set to 1 if the address is locally assigned. So far, the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with ‘FD’.

Scope of IPv6 Unicast Addresses

The scope of Link-local address is limited to the segment. Unique Local Address are locally global, but are not routed over the Internet, limiting their scope to an organization’s boundary. Global Unicast addresses are globally unique and recognizable. They shall make the essence of Internet v2 addressing.

3.2.2 Address Space

Q11. Explain about address space of IPv6.

Ans :

To simplify the address representation, IPv6 supports two types of abbreviations. Both abbreviations work with zeros. The first abbreviation allows us to skip leading zeros within a nibble while the second abbreviation allows us to drop the nibbles that contain only zeros. Since most IPv6 addresses contain long sequences of zeros, these two abbreviations can make writing IPv6 addresses a lot easier.

To understand how abbreviations work, let’s take an example. The following is the IPv6 address.

2001:0DB8:5002:AB41:0000:0000:0000:0801

The first form of abbreviation allows us to remove leading zeros within a nibble. After removing leading zeros from all nibbles, the above address could be abbreviated as the following.

2001:DB8:5002:AB41:0:0:0:801

The second form of abbreviation allows us to use a double colon to represent one or more consecutive sets of zero nibbles. Using this form of abbreviation, the above address can be further abbreviated as the following.

2001:DB8:5002:AB41::801

Two important rules must be followed when abbreviating an IPv6 address. First, you can’t abbreviate a zero that is not leading in the nibble. For example, you can’t abbreviate the address 2001:0DB8:5000: AB00:2300:0034:00A4:0801 as the 2001:0DB8:5:AB:23:34:A4:801. But, you can abbreviate this address as the 2001:DB8:5000:AB00:2300:34:A4:801.

Second, you can use only one double colon within an address representation. For example, you can abbreviate the address 2001:AB3:0:45CA:0:0:0:F5 as either 2001:AB3::45CA:0:0:0:F5 or 2001:AB3:0:45CA::F5. But you can't abbreviate this address as the 2001:AB3::45CA::F5. If you will use two double colons in an address, the address will be considered as an ambiguous address.

Calculating the full address from an abbreviated address

To calculate the full address from an abbreviate address, first, check whether the address has a double colon. If it has a double colon, determine how many 0 blocks are represented by the double colon. For this, count the number of blocks in the abbreviated address and subtract this number from 8. For example, in the address FF01::1, there are two blocks: FF01 and 1. The number of blocks expressed by the double colon (::) is 6 (8 blocks - 2 two blocks).

Once all 8 blocks are determined, count the number of hexadecimal digits in each block. Each block must contain 4 Hexadecimal digits. If any block contains less than 4 hexadecimal digits, add an equal number of zeros on the left side or in the leading position of the block.

Let's calculate the full address from the abbreviated example address.

Abbreviated example address

FF01::1

The address after removing abbreviated double-colon

FF01:0:0:0:0:0:0:1

The address after adding leading zeros in each block

FF01:0000:0000:0000:0000:0000:0000:0001

So the full address of the abbreviated address FF01::1 is the FF01:0000:0000:0000: 0000:0000: 0000:0001.

3.2.3 Packet Format and Extension Headers

Q12. Explain about IPv6 packet format and extension headers.

Ans : **(Imp.)**

The size of the IPv6 address is four times greater than the size of the IPv4 address but the IPv6 header size is only two times greater than the IPv4 header size.

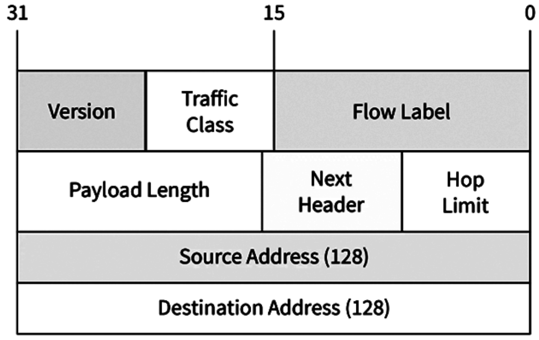
There is one fixed size header and zero or more than zero optional or extension headers in the IPv6 header. The fixed header keeps all the information that is important for the router. Optional information is kept in the extension header.

List of IPv6 Header Format Components

There are two main parts to the IPv6 data packet that is header and payload. The header of IPv6 is of fix length of 40 bytes which has the following fields:

Refer to the below image for the components of the IPv6 header

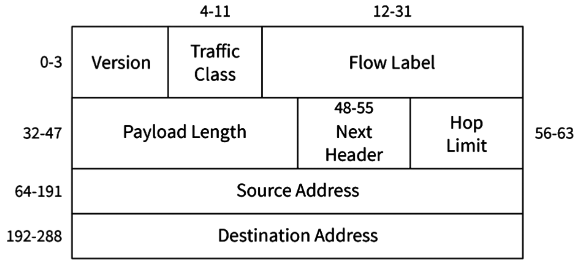
IPv6 Header Format



IPv6 Fixed Header

The size of the IPv6 fixed header is 40 bytes long and IPv6 header format consists of the following information:

Refer to the below image for the IPv6 fixed header



Version (4-bits) :

It shows the version of internet protocol we used, i.e. 0110

Traffic Class (8-bits) :

This is an 8-bit field in which 8 bits are divided into two parts. The most significant 6-bit is for the type of service so that the router will get to know about what services need to be provided to the given packet. And for Explicit Congestion Notification (ECN), the least significant 2-bit is used.

Flow Label (20-bits)

This 20-bit is required for maintaining the sequential flow of packets related to a particular communication. This field is also helpful in avoiding the reordering of packets. The source labels the sequence to help the router so that it can identify that a particular packet is related to a specific flow of data. It is generally used for real or streaming media.

Payload Length (16-bits)

This field is used to help the router in knowing how much information is stored in the payload of a particular packet.

Next Header (8-bits)

This field is used to represent the type of extension header or if the extension header is not present then it shows the Upper Layer PDU. The value for Upper Layer PDU is the same as that of values in IPv4.

Hop Limit (8-bits)

Hop limit is a field in a header that stops the header to go into an infinite loop in the network. It works the same as that of TTL in IPv4. When it passes a hop or router its value is decremented by 1. The packet is discarded when it reaches 0.

Source Address (128-bits)

This field provides the address from where the packet originates.

Destination Address (128-bits)

The destination address is the address of the packet's intended recipient.

IPv6 Extension Headers

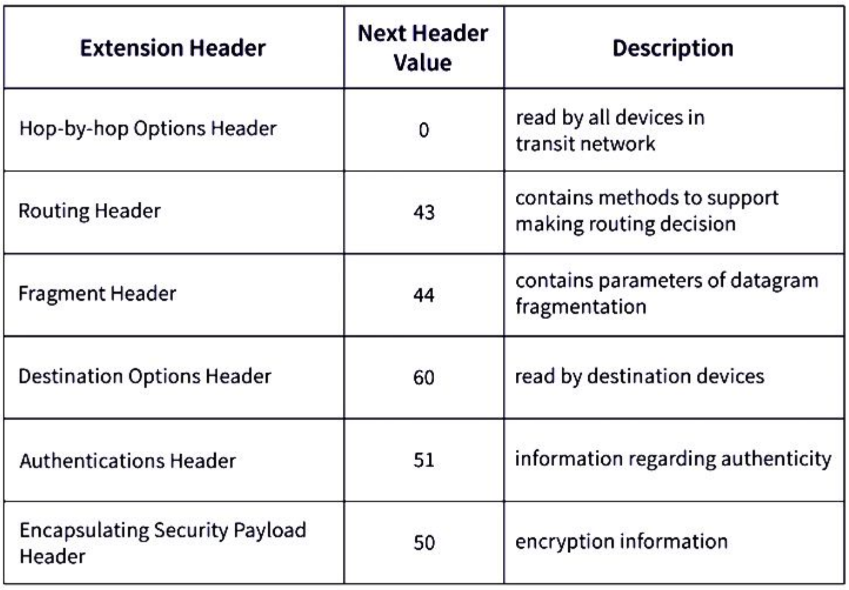
The fixed headers in IPv6 store only the information which is necessary, instead of the information that is rarely used or not needed. All this rarely used or not required information is stored in the form of the extension header and placed between the fixed header and the upper header. A distinct value is used for the identification of the extension header.

In the IPv6 header format, the Fixed Header's next header points to the header that is the first extension header, when the extension header is used. After this, if one or more header is present in the extension header then, the next header field of the first extension header points to the second extension header and follows this process for the rest of the extension headers. The next header field of the last extension header points to the Upper Layer header.

If there is a 59 value in the next header field then, it shows that there is no header after this header. And also not even the Upper Layer header is here after this header.

Following are some extension headers that must be supported according to RFC 2460:

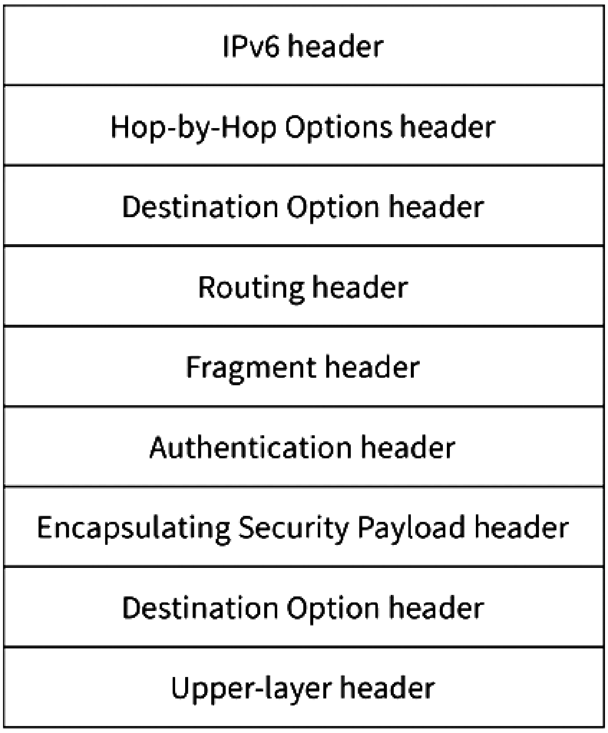
Refer to the below image for the extensions header supported by RFC 2460.



Extension Header	Next Header Value	Description
Hop-by-hop Options Header	0	read by all devices in transit network
Routing Header	43	contains methods to support making routing decision
Fragment Header	44	contains parameters of datagram fragmentation
Destination Options Header	60	read by destination devices
Authentications Header	51	information regarding authenticity
Encapsulating Security Payload Header	50	encryption information

The sequence of the Extension headers is given below :

Refer to the below image for the sequence of the extension header.



IPv6 header

Hop-by-Hop Options header

Destination Option header

Routing header

Fragment header

Authentication header

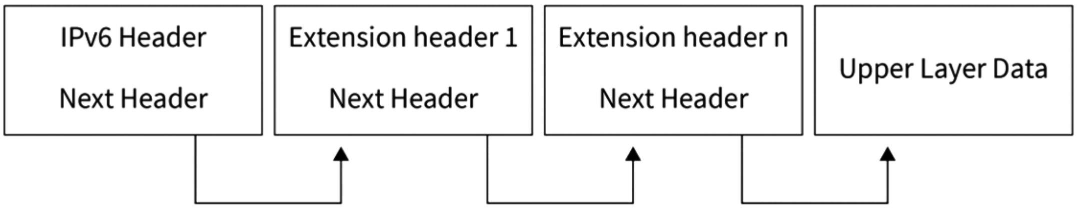
Encapsulating Security Payload header

Destination Option header

Upper-layer header

The headers that are arranged one after another in a linked list format are known as extension headers. The extension header is shown in the given figure.

Refer to the below image for the linked list format of the extension header.



Rules of Headers

The order of the header is defined by some predefined rules which are given below:

- If there is a **hop-by-hop** option then it must be after the **base** header of the IPv6 header.
- All headers except the destination header must be present once in the list.
- If the destination header appears before the routing header, then all the intermediate nodes that are in the routing header examine the destination header.
- If the destination header is present before the upper layer, then only the destination nodes will examine the destination header.

3.2.4 ICMP

Q13. Explain about ICMP Protocol.

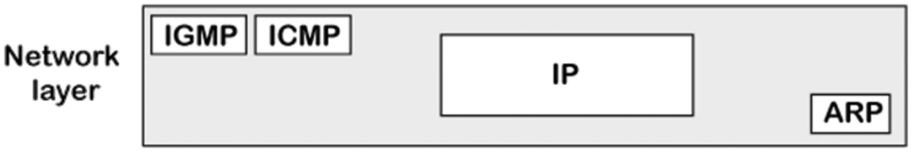
Ans :

The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

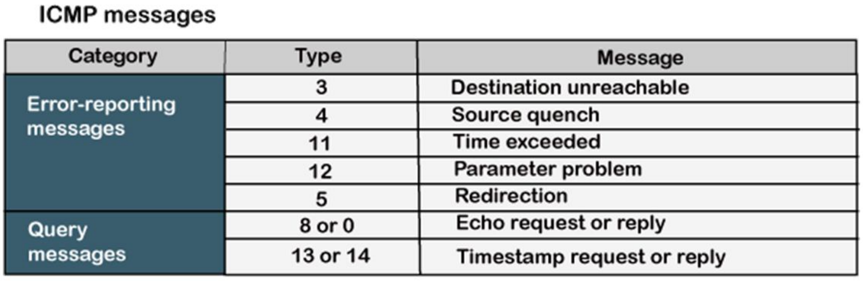
The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information. For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

The ICMP resides in the IP layer, as shown in the below diagram.



Messages

The ICMP messages are usually divided into two categories:



ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

- **Error-reporting messages**

The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.

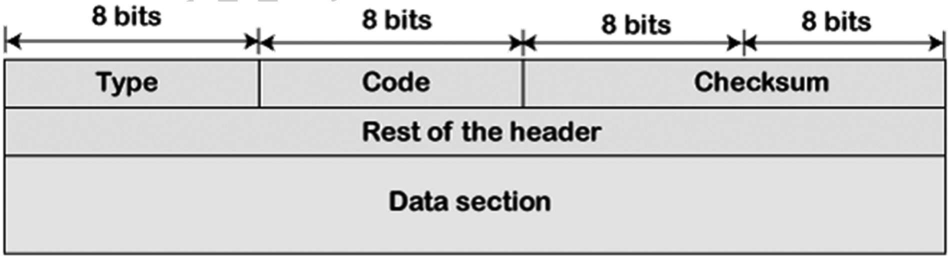
- **Query messages**

The query messages are those messages that help the host to get the specific information of another host. For example, suppose there are a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error **m**essage contains the type and the code. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields



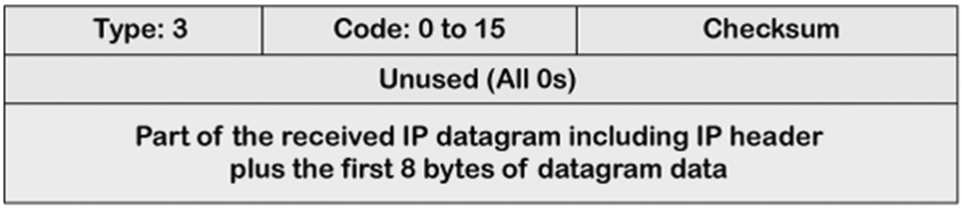
- **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- **Code:** It is an 8-bit field that defines the subtype of the ICMP message
- **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.

Types of Error Reporting messages

The error reporting messages are broadly classified into the following categories:

- **Destination unreachable**

The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.



Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above diagram shows the message format of the destination unreachable message. In the message format:

Type

It defines the type of message. The number 3 specifies that the destination is unreachable.

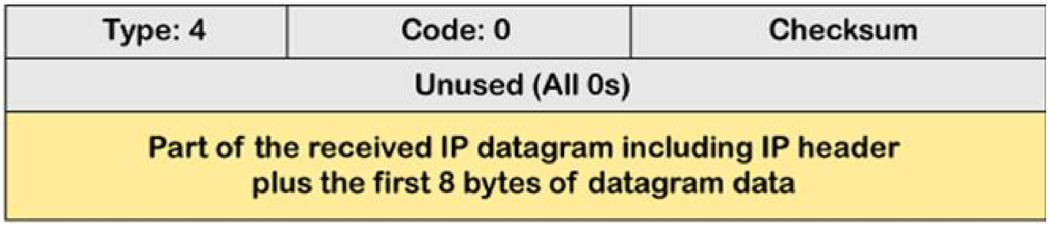
Code (0 to 15)

It is a 4-bit number which identifies whether the message comes from some intermediate router or the destination itself.

Sometimes the destination does not want to process the request, so it sends the destination unreachable message to the source. A router does not detect all the problems that prevent the delivery of a packet.

Source quench

There is no flow control or congestion control mechanism in the network layer or the IP protocol. The sender is concerned with only sending the packets, and the sender does not think whether the receiver is ready to receive those packets or is there any congestion occurs in the network layer so that the sender can send a lesser number of packets, so there is no flow control or congestion control mechanism. In this case, ICMP provides feedback, i.e., source quench. Suppose the sender resends the packet at a higher rate, and the router is not able to handle the high data rate. To overcome such a situation, the router sends a source quench message to tell the sender to send the packet at a lower rate.



Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above diagram shows the message format of the source quench message. It is a type 4 message, and code is zero.

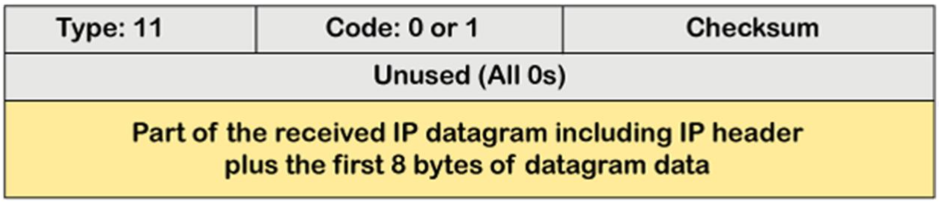
So, the sender must either stop or slow down the sending of datagrams until the congestion is reduced. The router sends one source-quench message for each datagram that is discarded due to the congestion in the network layer.

Time exceeded

Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop. The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.

Each of the MAC layers has different data units. For example, some layers can handle upto 1500 data units, and some can handle upto 300 units. When the packet is sent from a layer having 1500 units to the layer having 300 units, then the packet is divided into fragments; this process is known as fragmentation. These 1500 units are divided into 5 fragments, i.e., f1, f2, f3, f4, f5, and these fragments reach the destination in a sequence. If all the fragments are not reached to the destination in a set time, they discard all the received fragments and send a time-exceeded message to the original source.

In the case of fragmentation, the code will be different as compared to TTL. Let's observe the message format of time exceeded.



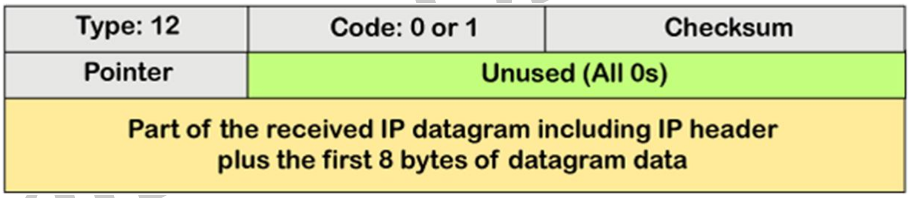
Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above message format shows that the type of time-exceeded is 11, and the code can be either 0 or 1. The code 0 represents TTL, while code 1 represents fragmentation. In a time-exceeded message, the code 0 is used by the routers to show that the time-to-live value is reached to zero.

The code 1 is used by the destination to show that all the fragments do not reach within a set time.

Parameter problems

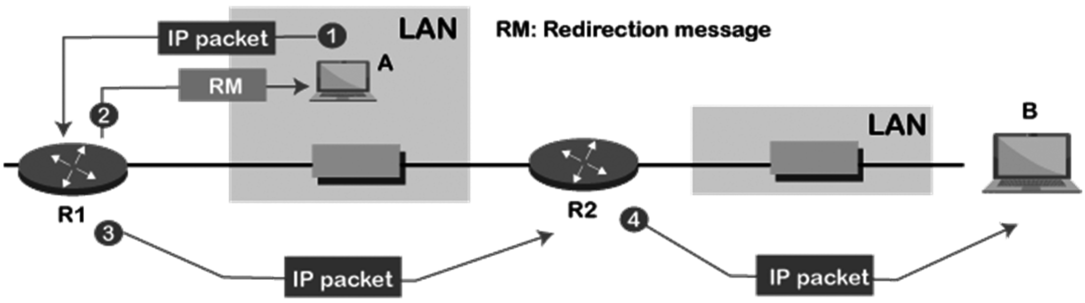
The router and the destination host can send a parameter problem message. This message conveys that some parameters are not properly set.



Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above diagram shows the message format of the parameter problem. The type of message is 12, and the code can be 0 or 1.

Redirection



When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message. For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and redirection message to A so that A can update its routing table.

ICMP Query Messages

The ICMP Query message is used for error handling or debugging the internet. This message is commonly used to ping a message.

Echo-request and echo-reply message

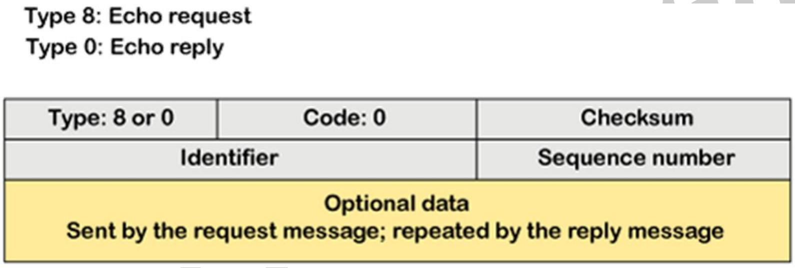
A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive". If the other host is alive, then it sends the echo-reply message. An echo-reply message is sent by the router or the host that receives an echo-request message.

Key points of Query messages

1. The echo-request message and echo-reply message can be used by the network managers to check the operation of the IP protocol. Suppose two hosts, i.e., A and B, exist, and A wants to communicate with host B. The A host can communicate to host B if the link is not broken between A and B, and B is still alive.

2. The echo-request message and echo-reply message check the host's reachability, and it can be done by invoking the ping command.

   The message format of echo-request and echo-reply message



Type 8: Echo request
Type 0: Echo reply

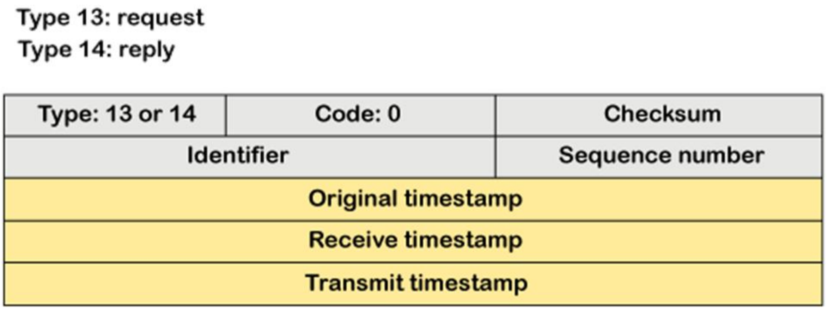
Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

The above diagram shows the message format of the echo-request and echo-reply message. The type of echo-request is 8, and the request of echo-reply is 0. The code of this message is 0.

Timestamp-request and timestamp-reply message

The timestamp-request and timestamp-reply messages are also a type of query messages. Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B. The computer B responds with a timestamp-reply message.

Message format of timestamp-request and timestamp-reply



Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		

The type of timestamp-request is 13, and the type of timestamp-reply is 14. The code of this type of message is 0.

Key points related to timestamp-request and timestamp-reply message

- It can be used to calculate the round-trip time between the source and the destination, even if the clocks are not synchronized.
- It can also be used to synchronize the clocks in two different machines if the exact transit time is known.

If the sender knows the exact transit time, then it can synchronize the clock. The sender asks the time on the receiver's clock, and then it adds the time and propagation delay. Suppose the time is 1:00 clock and propagation delay is 100 ms, then time would be 1:00 clock plus 100 ms.

Debugging tools

There are several tools used for debugging. In this topic, we will learn two tools that use ICMP for debugging. The two tools are ping and traceroute. We have learned about ping in echo-request and echo-reply messages that check whether the host or a router is alive or running.

Now we will take a look at the traceroute

Traceroute is a tool that tracks the route taken by a packet on an IP network from source to destination. It records the time taken by the packet on each hop during its route from source to destination. Traceroute uses ICMP messages and TTL values. The TTL value is calculated; if the TTL value reaches zero, the packet gets discarded. Traceroute uses small TTL values as they get quickly expired. If the TTL value is 1 then the message is produced by router 1; if the TTL value is 2 then the message is produced by router 2, and so on.

Let's understand the traceroute through an example

Suppose A and B are two different hosts, and A wants to send the packet to the host B. Between A and B, 3 routers exist. To determine the location of the routers, we use the traceroute tool.

TTL value =1

First, host A sends the packet to router 1 with TTL value 1, and when the packet reaches to router 1 then router reduces the value of TTL by one and TTL values becomes 0. In this case, router 1 generates the time-exceeded message and host A gets to know that router 1 is the first router in a path.

TTL value=2

When host A sends the packet to router 1 with TTL value 2, and when the packet reaches to router 1 then the TTL value gets decremented by 1 and the TTL value becomes 1. Then router 1 sends the packet to router 2, and the TTL value becomes 0, so the router generates a time-exceeded message. The host A gets to know that router 2 is the second router on the path.

TTL value=3

When host A sends the packet to router 1 with TTL value 3, then the router decrements its value by one, and the TTL value becomes 2. Then, router 1 sends the packet to router 2, and the TTL value becomes 1. Then, router 2 sends the packet to router 3, and the TTL value becomes 0. As TTL value becomes 0, router 3 generates a time-exceeded message. In this way, host A is the third router on a path.

3.2.5 IGMP

Q14. Explain about IGMP protocol.

Ans :

IGMP is an abbreviated form of Internet Group Management Protocol(IGMP). Mainly the Internet Protocol can be involved in the two types of communication i.e, Unicasting and multicasting. IGMP is one of the necessary but not the efficient protocol that is involved in Multicasting.

IGMP is basically a companion of Internet Protocol (IP).

IGMP is not a multicasting routing protocol but it is a protocol that manages the group membership. This protocol mainly helps the multicast routers in order to create and update a list of loyal members that are related to each router interface.

This protocol is used in streaming videos, gaming, or web conferencing tools.

IGMP Messages

There are two versions of IGMP: IGMPv1 and IGMPv2.

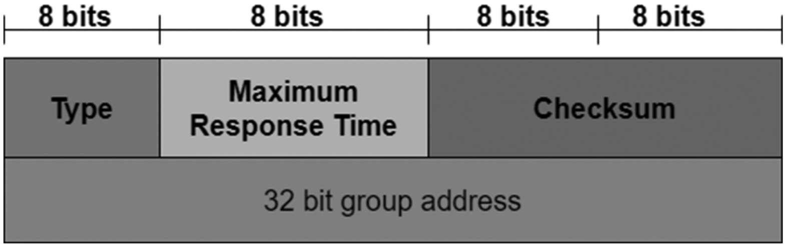
The version IGMPv2 has three types of messages:

- The Query
- The Membership report
- The Leave report.

There are two types of Query messages: General and Special

Message Format

Let us now take a look at the format of IGMP(Version 2):



Type

This is an 8-bit field and is mainly used to define the type of the message. The value of the type can be in both hexadecimal as well as binary notations.

Maximum Response Time

The size of this field is also 8 bit and it mainly defines the amount of time in which query must be answered. The value of this field is nonzero in the query message; while its value is zero in the other two types.

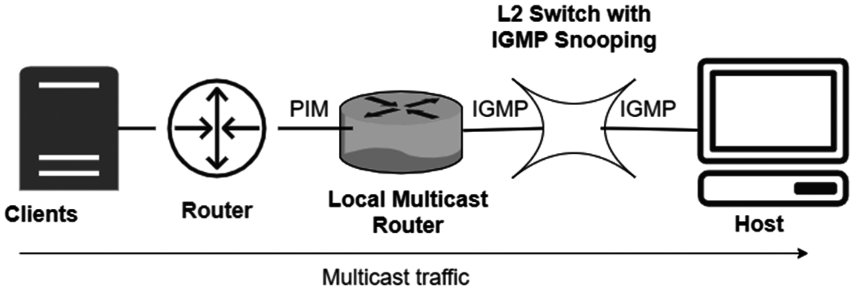
Working of IGMP

This protocol mainly works on the device that has the capability of handling multiple groups and used for dynamic multicasting; these devices mainly allow the host in order to join or leave the membership in the multicast group.

Also, these devices are allowed to add and remove the clients from the group.

IGMP protocol mainly operates in between the host and local multicast router

At the time when there is a creation of the multicast group, the multicast group address is in the range of class D (224-239) IP addresses and is forwarded as the destination IP address in the packet.



L2 means level-2 devices like switches; these are mainly used in between the host and multicast router for the snooping of IGMP.

IGMP snooping

It is a process that is used to listen to the IGMP network traffic in a controlled manner.

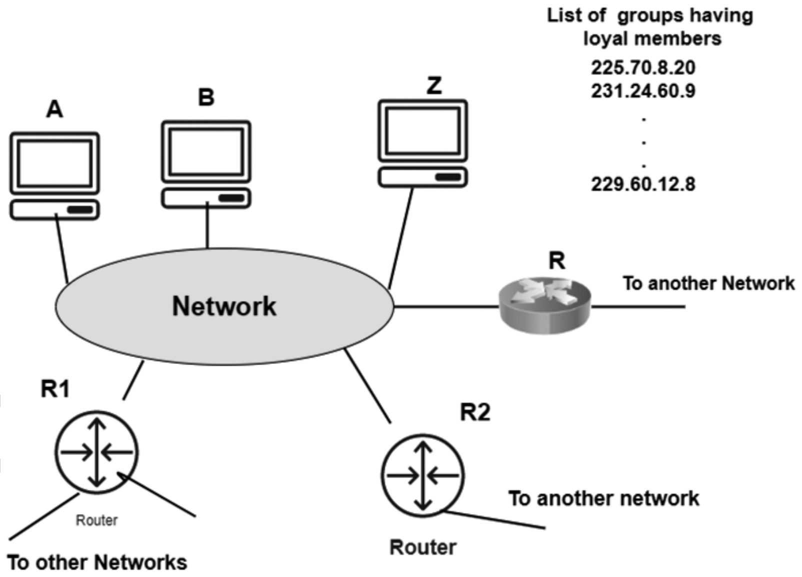
The switch mainly receives the message from the host and then forwards the membership report mainly to the local multicast router. After that, the multicast traffic is then further forwarded to remote routers from local multicast routers using PIM (Protocol Independent Multicast) protocol so that the clients can receive the message/data packets.

If the Clients wish to join the network then they can send a join message in the query and then the switch intercepts the message and then adds the ports of clients to its multicast routing table.

IGMP Operation

The Internet Group Management Protocol operates locally. The Multicast router that is connected to the network mainly has a list of multicast addresses of the group with at least one loyal member in that network. And for each group, there is mainly one router that has the duty of distributing the multicast packets destined for that group.

This simply indicates that in the case if there are three multicast routers connected to a network then their list of groupids are mutually exclusive.



Given below are the operations of IGMP:

Joining a Group

- In this operation, both the host and the router can join a group. Whenever a process on the host wants to join a group then it simply sends the request to the host. After that, the host then adds the name of the process and the name of the group to its list.
- In case, if this is the first entry of that particular group, then the host sends the membership report message to the multicast router of the group.
- And if the entry is not the first entry then there is no need of sending such a message.

Leaving a group

- Whenever the host finds that there is no process that is interested in the group then it mainly leaves a report message.

- The membership is not disinfected by the multicast router of the group, rather than it immediately transmits the query packets repeatedly to see if anyone is still interested or not.
- And in case if it gets the response in the form of a membership report message then the membership of the host or network is preserved.
- **Monitoring Membership:** Mainly the general query message does not define a particular group.
- **Delayed Response:** In order to prevent unnecessary traffic, the IGMP mainly makes use of a delayed response strategy.

Advantages of IGMP

The listed below are some of the benefits offered by the IGMP:

- With the help of this protocol, the bandwidth is utilized efficiently aa because all the shared links are connected.
- Using this protocol, the host can immediately leave a multicast group and then join another group.
- The performance of this protocol is optimized as there is no transmission of junk packets to the host.

Disadvantages of IGMP

Given below are some of the drawbacks of the IGMP :

- During filtering and security, it does not offers good efficiency.
- This protocol is vulnerable to Denial of Service (DoS) attacks.
- Network congestion can occur due to a lack of TCP.

3.2.6 ARP

Q15. What is ARP? Explain about it.

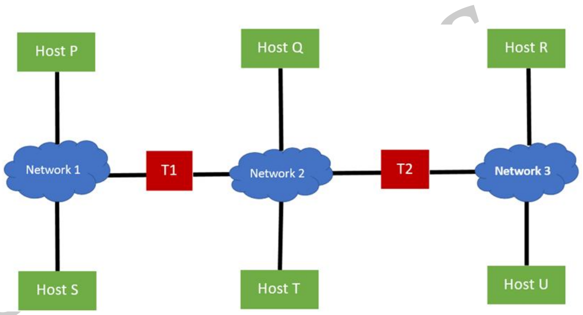
Ans :

Address Resolution Protocol (ARP) is an important protocol of the network layer in the OSI model, which helps find the MAC (Media Access Control) address given the system's IP address. The ARP's main task is to convert the 32-bit IP address (for IPv4) to a 48-bit MAC address.

This protocol is mostly used to determine the hardware (MAC) address of a device from an IP address. It is also used when one device wants to communicate with some other device on a local network. The full form of ARP is Address Resolution Protocol.

Working Mechanism

All OS in an IPv4 network keeps an ARP cache. When the host requests a MAC address to send a packet to another host in the LAN, it checks its ARP cache to check that the MAC address translation already presents.



Let us understand this concept with an example:

- Hosta P resolves protocol address for host U for protocol messages from an application on P sent to U.
- P does not resolve a protocol address for host U
- By using the internet layer, host P delivers to host U by routing through T1 and T2.
- Host P resolves the T1 hardware address.
- Network layer on host P passes packet containing destination protocol address for U for delivery to T1
- T1 delivers the packet to T2 which in turn forwards the packet to Host U.

Address Resolution Methods

Association between a protocol address and a hardware address is known as binding.

There are three techniques used for this purpose:

- **Table lookup:** Bindings stored in memory with protocol address as the key. It uses the data link layer to check the protocol address to find the hardware address.
- **Dynamic:** This type of network messaging method is used for "just-in-time" resolution. Data link layer sends message requests in a hardware address. destination responds.
- **Closed-form computation:** In this method, a protocol address is based on a hardware address. Data link layer derives the hardware address from the protocol address.

Types

Here are four types of Address Resolution Protocol, which is given below:

1. Proxy ARP
2. Gratuitous ARP
3. Reverse ARP
4. Inverse ARP

1. Proxy ARP

In the Proxy ARP method, Layer 3 devices can respond to ARP requests. This ARP type is configured router will respond to the target IP address and maps the router's MAC address with the target IP address and sender when it is reached to its destination.

2. Gratuitous ARP

Gratuitous is another type of ARP request of the host. This type of ARP request helps the network to identify the duplicate IP address. Therefore, when an ARP request is sent by a router or switch to get its IP address, no ARP responses are received so that no other nodes can use the IP address allocated to that switch or router.

3. Reverse ARP (RARP)

Reverse ARP, also now called RARP, is a type of ARP networking protocol which is used by the client system in a LAN to request its IPv4 address from the ARP router table. The network admin mostly creates a table in the gateway-router, which helps determine the MAC address to that specific IP address.

4. Inverse ARP (InARP)

Inverse ARP is also called InARP, is a type of ARP used to find the nodes' IP of addresses from the data link layer addresses. InARP is widely used for ATM networks frame relays where Layer 2 virtual circuit addressing acquired from Layer 2 signaling.

ARP Header

Hardware Type		Protocol Type
Hardware Length	Protocol Length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 4 bytes for IP)		
Target Protocol address (For example, 4 bytes for IP)		

ARP header

- **Hardware Type:** It is 1 for Ethernet.
- **Protocol Type:** It is a protocol used in the network layer.
- **Hardware Address Length:** It is the length in bytes so that it would be 6 for Ethernet.
- **Protocol Address Length:** Its value is 4 bytes.
- **Operation Code:** indicates that the packet is an ARP Request (1) or an ARP Response (2).
- **Senders Hardware Address:** It is a hardware address of the source node.
- **Senders Protocol Address:** It is a layer 3 address of the source node.
- **Target Hardware Address:** It is used in a RARP request, which response impact both the destination's hardware and layer 3 addresses.
- **Target Protocol Address:** It is used in an ARP request when the response carries both layer 3 addresses and the destination's hardware.

Advantages of using ARP

Here are the pros/benefits of using ARP

- If you are using ARP, then MAC addresses can easily be known if you know the IP address of the same system.
- End nodes should not be configured to "know" MAC addresses. It can be found when needed.
- ARP's goal is to enable each host on a network that allows you to build up a mapping between IP addresses and physical addresses.
- The set of mappings or table stored in the host is called ARP table or ARP cache.

3.2.7 RARP

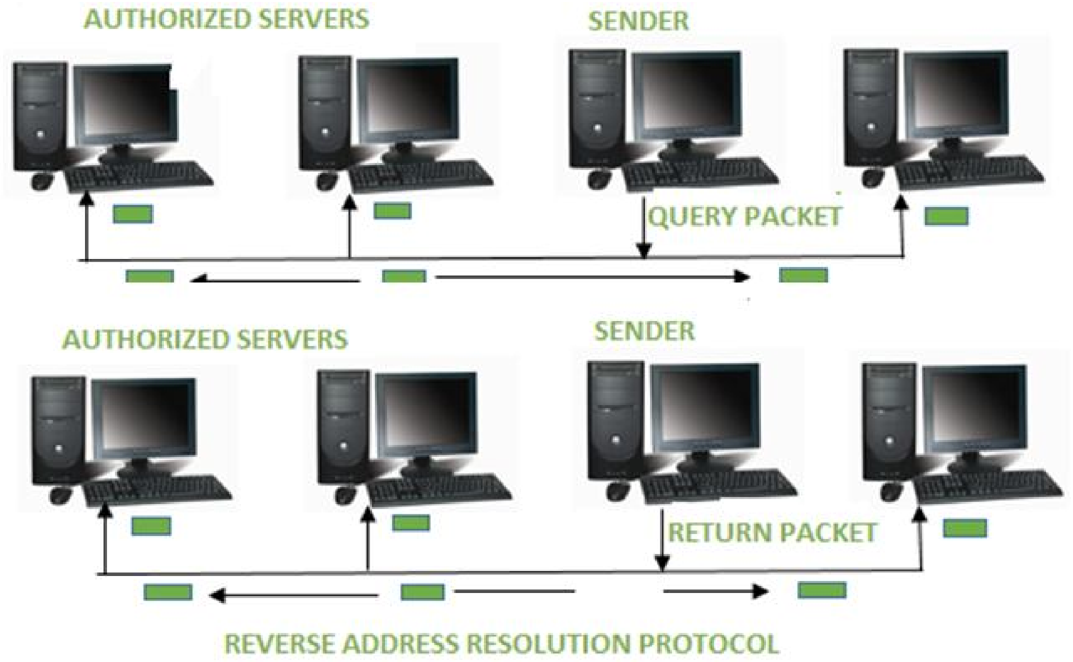
Q16. Explain about Reverse Address Resolution Protocol

Ans :

RARP is abbreviation of Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

This protocol is used to communicate data between two points in a server. The client doesn't necessarily need prior knowledge the server identities capable of serving its request. Media Access Control (MAC) addresses requires individual configuration on the servers done by an administrator. RARP limits to the serving of IP addresses only.

When a replacement machine is set up, the machine may or might not have an attached disk that may permanently store the IP Address so the RARP client program requests IP Address from the RARP server on the router. The RARP server will return the IP address to the machine under the belief that an entry has been setup within the router table.



History

RARP was proposed in 1984 by the university Network group. This protocol provided the IP Address to the workstation. These diskless workstations were also the platform for the primary workstations from Sun Microsystems.

Working

The RARP is on the Network Access Layer and is employed to send data between two points in a very network.

Each network participant has two unique addresses:- IP address (a logical address) and MAC address (the physical address).

The IP address gets assigned by software and after that the MAC address is constructed into the hardware.

The RARP server that responds to RARP requests, can even be any normal computer within the network. However, it must hold the data of all the MAC addresses with their assigned IP addresses. If a RARP request is received by the network, only these RARP servers can reply to it. The info packet needs to be sent on very cheap layers of the network. This implies that the packet is transferred to all the participants at the identical time.

The client broadcasts a RARP request with an Ethernet broadcast address and with its own physical address. The server responds by informing the client its IP address.

Q17. How is RARP different from ARP ?

Ans :

Sl.No.	RARP	ARP
1.	RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
2.	In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
3.	The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
4.	It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

Q18. Sate the uses and disadvantage of RARP?

Ans :

Uses of RARP

RARP is used to convert the Ethernet address to an IP address. It is available for the LAN technologies like FDDI, token ring LANs, etc.

Disadvantages

The Reverse Address Resolution Protocol had few disadvantages which eventually led to its replacement by BOOTP and DHCP. Some of the disadvantages are listed below:

- The RARP server must be located within the same physical network.
- The computer sends the RARP request on very cheap layer of the network. Thus, it's unattainable for a router to forward the packet because the computer sends the RARP request on very cheap layer of the network.
- The RARP cannot handle the subnetting process because no subnet masks are sent. If the network is split into multiple subnets, a RARP server must be available with each of them.
- It isn't possible to configure the PC in a very modern network.
- It doesn't fully utilize the potential of a network like Ethernet

3.3 Congestion Control and Resource Allocation

3.3.1 Problem

Q19. What is congestion control problem for assigning resources

Ans :

The main problem here is , how to effectively and fairly allocate resources among a collection of competing users. The resources being shared include the bandwidth of the links and the buffers on the routers or switches where packets are queued awaiting transmission. Packets *contend* at a router for the use of a link, with each contending packet placed in a queue waiting its turn to be transmitted over the link. When too many packets are contending for the same link, the queue fills and two undesirable things happen: packets experience increased end-to-end delay, and in the worst case, the queue overflows and packets have to be dropped. When long queues persist and drops become common, the network is said to be *congested*. Most networks provide a *congestion-control* mechanism to deal with just such a situation.

Congestion control and resource allocation are two sides of the same coin. On the one hand, if the network takes an active role in allocating resources - for example, scheduling which virtual circuit gets to use a given physical link during a certain period of time - then congestion may be avoided, thereby making congestion control unnecessary. Allocating network resources with any precision is difficult, however, because the resources in question are distributed throughout the network; multiple links connecting a series of routers need to be scheduled. On the other hand, you can always let packet sources send as much data as they want and then recover from congestion should it occur. This is the easier approach, but it can be disruptive because many packets may be discarded by the network before congestion can be controlled.

Congestion control and resource allocation involve both hosts and network elements such as routers. In network elements, various queuing disciplines can be used to control the order in which packets get transmitted and which packets get dropped. The queuing discipline can also segregate traffic to keep one user's packets from unduly affecting another user's packets. At the end hosts, the congestion-control mechanism paces how fast sources are allowed to send packets. This is done in an effort to keep congestion from occurring in the first place and, should it occur, to help eliminate the congestion.

3.3.2 ISSUES

Q20. What are the issues in allocating resources ? Write about it.

Ans : **(Imp.)**

Resource allocation is partially implemented in the routers, switches, and links inside the network and partially in the transport protocol running on the end hosts. End systems may use signalling protocols to convey their resource requirements to network nodes, which respond with information about resource availability.

It is also important to understand the difference between flow control and congestion control. Flow control involves keeping a fast sender from overrunning a slow receiver

Network Model

We begin by defining three salient features of the network architecture.

Packet-Switched Network

We consider resource allocation in a packet-switched network (or internet) consisting of multiple links and switches (or routers). Since most of the mechanisms described in this chapter were designed for use on the Internet, and therefore were originally defined in terms of routers rather than switches, we use the term *router* throughout our discussion. The problem is essentially the same, whether on a network or an internetwork.

In such an environment, a given source may have more than enough capacity on the immediate outgoing link to send a packet, but somewhere in the middle of a network its packets encounter a link that is being used by many different traffic sources. Figure 1 illustrates this situation—two high-speed links are feeding a low-speed link. This is in contrast to shared-access networks like Ethernet and wireless networks, where the source can directly observe the traffic on the network and decide accordingly whether or not to send a packet.

Connectionless Flows

We assume that the network is essentially connectionless, with any connection-oriented service implemented in the transport protocol that is running on the end hosts

This is precisely the model of the Internet, where IP provides a connectionless datagram delivery service and TCP implements an end-to-end connection abstraction.

The major shortcoming of this approach is that it leads to an underutilization of resources—buffers reserved for a particular circuit are not available for use by other traffic even if they were not currently being used by that circuit.

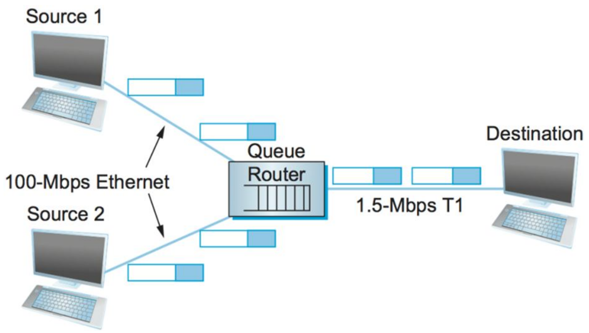


Fig.1: A potential bottleneck router

We need to qualify the term *connectionless* because our classification of networks as being either connectionless or connection oriented is a bit too restrictive; there is a gray area in between. In particular, the assumption that all datagrams are completely independent in a connectionless network is too strong. The datagrams are certainly switched independently, but it is usually the case that a stream of datagrams between a particular pair of hosts flows through a particular set of routers. This idea of a *flow*—a sequence of packets sent between a source/destination pair and following the same route through the network—is an important abstraction in the context of resource allocation.

One of the powers of the flow abstraction is that flows can be defined at different granularities. For example, a flow can be host-to-host (i.e., have the same source/destination host addresses) or process-to-process (i.e., have the same source/destination host/port pairs). In the latter case, a flow is essentially the same as a channel, as we have been using that term throughout this book. The reason we introduce a new term is that a flow is visible to the routers inside the network, whereas a channel is an end-to-end abstraction. Figure 153 illustrates several flows passing through a series of routers.

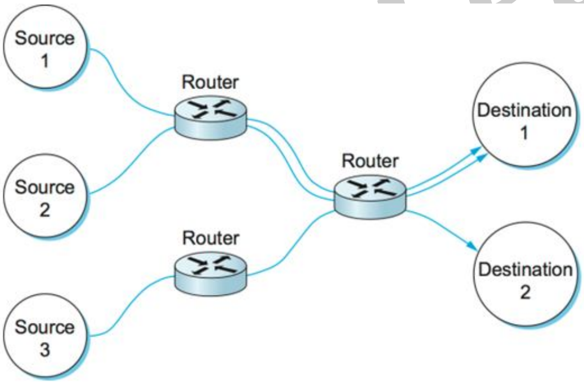


Fig.: Multiple flows passing through a set of routers

Because multiple related packets flow through each router, it sometimes makes sense to maintain some state information for each flow, information that can be used to make resource allocation decisions about the packets that belong to the flow. This state is sometimes called *soft state*. The main difference between soft state and hard state is that soft state need not always be explicitly created and removed by signalling. Soft state represents a middle ground between a purely connectionless network that maintains *no* state at the routers and a purely connection-oriented network that maintains hard state at the routers. In general, the correct operation of the network does not depend on soft state being present (each packet is still routed correctly without regard to this state), but when a packet happens to belong to a flow for which the router is currently maintaining soft state, then the router is better able to handle the packet.

Note that a flow can be either implicitly defined or explicitly established. In the former case, each router watches for packets that happen to be traveling between the same source/destination pair- the router does this by inspecting the addresses in the header - and treats these packets as belonging to the same flow for the purpose of congestion control. In the latter case, the source sends a flow setup message across the network, declaring that a flow of packets is about to start.

Taxonomy

There are countless ways in which resource allocation mechanisms differ, so creating a thorough taxonomy is a difficult proposition. We describe three dimensions along which resource allocation mechanisms can be characterized.

Router-Centric versus Host-Centric

Resource allocation mechanisms can be classified into two broad groups: those that address the problem from inside the network (i.e., at the routers or switches) and those that address it from the edges of the network (i.e., in the hosts, perhaps inside the transport protocol).

In a router-centric design, each router takes responsibility for deciding when packets are forwarded and selecting which packets are to be dropped, as well as for informing the hosts that are generating the network traffic how many packets they are allowed to send. In a host-centric design, the end hosts observe the network conditions (e.g., how many packets they are successfully getting through the network) and adjust their behavior accordingly.

Reservation-Based versus Feedback-Based

A second way that resource allocation mechanisms are sometimes classified is according to whether they use *reservations* or *feedback*. In a reservation-based system, some entity (e.g., the end host) asks the network for a certain amount of capacity to be allocated for a flow. Each router then allocates enough resources (buffers and/or percentage of the link's bandwidth) to satisfy this request. If the request cannot be satisfied at some router, because doing so would overcommit its resources, then the router rejects the reservation. This is analogous to getting a busy signal when trying to make a phone call. In a feedback-based approach, the end hosts begin sending data without first reserving any capacity and then adjust their sending rate according to the feedback they receive. This feedback can be either explicit or implicit.

Window Based versus Rate Based

A third way to characterize resource allocation mechanisms is according to whether they are window based or rate based. This is one of the areas, noted above, where similar mechanisms and terminology are used for both flow control and congestion control. Both flow-control and resource allocation mechanisms need a way to express, to the sender, how much data it is allowed to transmit. There are two general ways of doing this: with a *window* or with a *rate*. We have already seen window-based transport protocols, such as TCP, in which the receiver advertises a window to the sender. This window corresponds to how much buffer space the receiver has, and it limits how much data the sender can transmit; that is, it supports flow control. A similar mechanism - window advertisement - can be used within the network to reserve buffer space (i.e., to support resource allocation). TCP's congestion-control mechanisms are window based.

Evaluation Criteria

The final issue is one of knowing whether a resource allocation mechanism is good or not. Recall that in the problem statement at the start of this chapter we posed the question of how a network effectively and fairly allocates its resources.

There re two ways by which a resource allocation scheme can be evaluated.

Effective Resource Allocation

A good starting point for evaluating the effectiveness of a resource allocation scheme is to consider the two principal metrics of networking: throughput and delay. Clearly, we want as much throughput and as little delay as possible. Unfortunately, these goals are often somewhat at odds with each other. One sure way for a resource allocation algorithm to increase throughput is to allow as many packets into the network as possible, so as to drive the utilization of all the links up to 100%. We would do this to avoid the possibility of a link becoming idle because an idle link necessarily hurts throughput. The problem with this strategy is that increasing the number of packets in the network also increases the length of the queues at each router. Longer queues, in turn, mean packets are delayed longer in the network.

This ratio is sometimes referred to as the *power* of the network:

Power = Throughput / Delay

Fair Resource Allocation

The effective utilization of network resources is not the only criterion for judging a resource allocation scheme. We must also consider the issue of fairness. However, we quickly get into murky waters when we try to define what exactly constitutes fair resource allocation. For example, a reservation-based resource allocation scheme provides an explicit way to create controlled unfairness. With such a scheme, we might use reservations to enable a video stream to receive 1 Mbps across some link while a file transfer receives only 10 kbps over the same link.

In the absence of explicit information to the contrary, when several flows share a particular link, we would like for each flow to receive an equal share of the bandwidth. This definition presumes that a *fair* share of bandwidth means an *equal* share of bandwidth. But, even in the absence of reservations, equal shares may not equate to fair shares.

3.3.3 Queuing

Q21. Explain about the queuing algorithms in congestion control.

Ans : **(Imp.)**

The queuing algorithm can be thought of as allocating both bandwidth and buffer space .It also directly affects the latency experienced by a packet by determining how long a packet waits to be transmitted.

There are two common queuing algorithms - first-in, first-out (FIFO) and fair queuing (FQ)/

FIFO

The idea of FIFO queuing, also called first-come, first-served (FCFS) queuing, is simple: The first packet that arrives at a router is the first packet to be transmitted

This is illustrated in Figure 1(a), which shows a FIFO with "slots" to hold up to eight packets. Given that the amount of buffer space at each router is finite, if a packet arrives and the queue (buffer space) is full, then the router discards that packet, as shown in Figure 1(b). This is done without regard to which flow the packet belongs to or how important the packet is. This is sometimes called *tail drop*, since packets that arrive at the tail end of the FIFO are dropped.

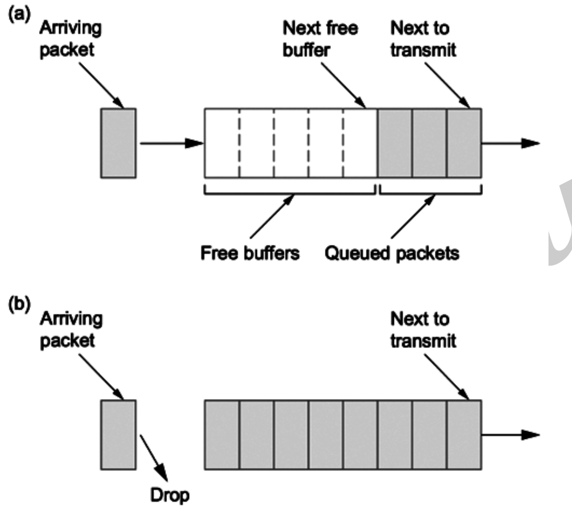


Fig.: FIFO queuing (a), and tail drop at a FIFO queue (b)

Note that tail drop and FIFO are two separable ideas. FIFO is a scheduling discipline - it determines the order in which packets are transmitted. Tail drop is a drop policy - it determines which packets get dropped. Because FIFO and tail drop are the simplest instances of scheduling discipline and drop policy, respectively, they are sometimes viewed as a bundle.

FIFO with tail drop, as the simplest of all queuing algorithms, is the most widely used in Internet routers at the time of writing. This simple approach to queuing pushes all responsibility for congestion control and resource allocation out to the edges of the network. Thus, the prevalent form of congestion control in the Internet currently assumes no help from the routers: TCP takes responsibility for detecting and responding to congestion.

A simple variation on basic FIFO queuing is priority queuing. The idea is to mark each packet with a priority; the mark could be carried, for example, in the IP header, as we'll discuss in a later section. The routers then implement multiple FIFO queues, one for each priority class. The router always transmits packets out of the highest-priority queue if that queue is nonempty before moving on to the next priority queue. Within each priority, packets are still managed in a FIFO manner.

Fair Queuing

This algorithm finds its role incontrolling congestion in datagram. Itwas found out that fair queuing provides several important advantages over the usual firstcome-first-serve queuing algorithm .

Congestion in the datagram networks can be controlled in two ways:

1. At the source, where flow control algorithms vary the rate at which source sendspackets.
2. At the gateway, where routing and queuing algorithms control the congestion. We are going to assume that we are using the best flow control algorithms and hence in this paper we are going to discuss only about queuing algorithms.

Queuing algorithms can be thought of as allocating three nearly independent quantities: bandwidth (which packets get transmitted), promptness (when do those packets get transmitted), and buffer space (which packets are discarded by the gateway).

Before this first-come-first-serve (FCFS) was the most common algorithm. But this algorithm was fraught with malfunctions such as allocation of higher bandwidth to a source, sending packets at sufficiently high speed. So in a fair queuing algorithm in which gateways maintain separate queues for packets from each individual source and serviced them in a round-robin manner.

In circuit switched networks where there is explicit buffer reservation and uniform packet size, it has been established that round robin service disciplines allocate bandwidth fairly. But in case of other networks, a source using long packets gets more bandwidth than one using short bandwidth, so bandwidth is not allocated fairly.

fair allocation

Let's consider allocation of a single resource among N users as an example. Assume there is an amount total of this resource and each user requests an amount 0i and, under a particular allocation, receives an amount ìi. The max-min fairness criterion states that an allocation is fairif (1) no user receives more than it requests, (2) no other allocation scheme satisfying condition 1 has a higher minimum allocation, and condition 2 remains recursively true as we remove the minimal user and reduce the total resource accordingly,

μtotal $\leftarrow$ μtotal - μmin.

This condition reduces to μi = MIN(μfair, μi) in the simple example, with μfair, the fair share, being set so that μtotal $= \sum_{1}^{N} = 1\mu_{1\ i}$

Allocation on the basis of source-destination pairs, or conversations, will constitute a user.

Definition of Algorithm

Owing to varying packet-sizes, fair allocation of bandwidths is not an easy task. To see how this unfairness can be avoided, a hypothetical service discipline where transmission occurs in a bit by bit round robin fashion.

In this the bandwidth is allocated fairly since at every instant in time, each conversation is receiving its fair share. Let R(t) denote the number of rounds made in the round-robin service discipline up to time t (R(t) is a continuous function, with the fractional part indicating partially completed rounds). Let Nac(t) denote the number of active conversations, i.e. those that have bits in their queue at time t. Then, $\frac{\partial R}{\partial t} = \frac{\mu}{N_{ac}(t)}$, where μ is the

Line speed of the gateway's outgoing line (we will, for convenience, work in units such that μ= 1). A packet of size P whose first bit ge ts serviced at time to will have its last bit serviced P rounds later, at time t such that R(t) = R(to) + P. Let tt_ be the time that packet i belonging to conversation _ arrives at the gateway, and define the numbers Si_ and Fi_ as the values of R(t) when the packet started and finished service. With Pi_ denoting the size of the packet, the following relations hold: $F_i^{\alpha} = S_i^{\alpha} + P_i^{\alpha}$ and S_i = MAX(Fi-1, R(t_i^{α})).

Sending packets in a bit-by-bit round robin fashion while satisfying our requirements for an adequate queuing algorithm, is obviously unrealistic. This impractical algorithm is tried to be emulated in a practical packet-by-packet transmission scheme. A natural way to emulate the bit-by-bit round-robin algorithm is to let the quantities F_i^{α} define the sending order of the packets. Our packet-by-packet transmission algorithm is simply defined by the rule that, whenever a packet finishes transmission, the next packet sent is the one with the smallest value of F_i^{α}. In a preemptive version of this algorithm, newly arriving packets whose finishing number F_i^{α} is smaller than that of the packet currently in transmission preempt the transmitting packet.

Promptness allocation must be based solely on data already available at the gateway. One such allocation strategy is to give more promptness (less delay) to users who utilize less than their fair share of bandwidth. Separating the promptness allocation from the bandwidth allocation can be accomplished by introducing a nonnegative parameter :, and defining a new quantity, the bid B_i, via $B_i^a = P_i^a$ + MAX(Fi-1^a, R(t_i^a)-d). The quantities R(t), Nac(t), S_i^a and F_i remain as before, but now the sending order is determined by the B's, not the F's. The asymptotic band width allocation is independent odd. since the F's control the bandwidth allocation, but the algorithm gives slightly faster service to packets that arrive at an inactive conversation.

3.3.4 TCP

Q22. Explain about TCP algorithms for congestion control.

Ans : **(Imp.)**

TCP reacts to congestion by reducing the sender window size.

The size of the sender window is determined by the following two factors-

Receiver Window Size-

Receiver window size is an advertisement of-

"How much data (in bytes) the receiver can receive without acknowledgment?"

- Sender should not send data greater than receiver window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to receiver window size.
- Receiver dictates its window size to the sender through TCP Header.

2. Congestion Window

- Sender should not send data greater than congestion window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to congestion window size.
- Different variants of TCP use different approaches to calculate the size of congestion window.
- Congestion window is known only to the sender and is not sent over the links.

So, always-

Sender window size = Minimum (Receiver window size, Congestion window size)

TCP Congestion Policy

TCP's general policy for handling congestion consists of following three phases-

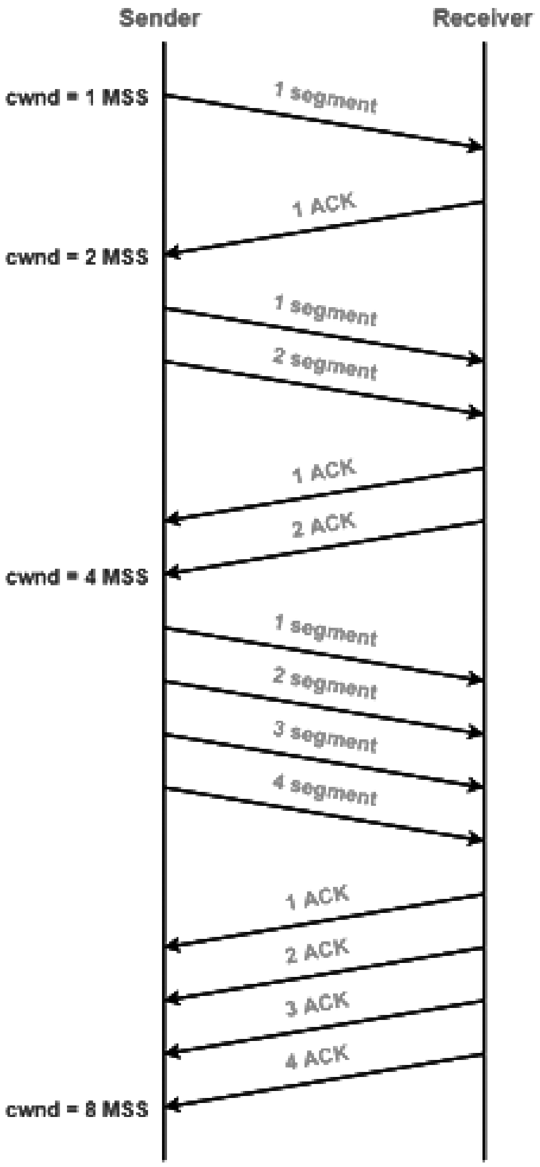
1. Slow Start Phase

- Initially, sender sets congestion window size = Maximum Segment Size (1 MSS).
- After receiving each acknowledgment, sender increases the congestion window size by 1 MSS.
- In this phase, the size of congestion window increases exponentially.

The followed formula is-

Congestion window size = Congestion window size + Maximum segment size

This is shown below-



(cwnd = congestion window size)

- After 1 round trip time, congestion window size = $(2)^1$ = 2 MSS
- After 2 round trip time, congestion window size = $(2)^2$ = 4 MSS
- After 3 round trip time, congestion window size = $(2)^3$ = 8 MSS and so on.

This phase continues until the congestion window size reaches the slow start threshold.

Threshold

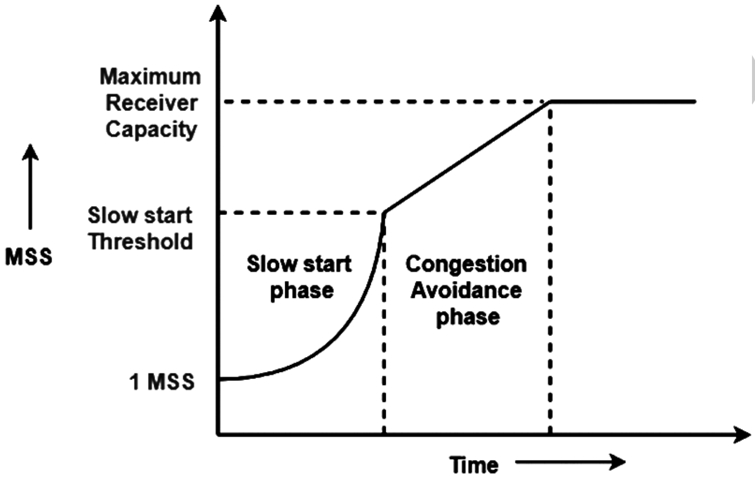
= Maximum number of TCP segments that receiver window can accommodate / 2

= (Receiver window size / Maximum Segment Size) / 2

2. Congestion Avoidance Phase-

After reaching the threshold,

- Sender increases the congestion window size linearly to avoid the congestion.
- On receiving each acknowledgments, sender increments the congestion window size by 1.
- The followed formula is- Congestion window size = Congestion window size + 1
- This phase continues until the congestion window size becomes equal to the receiver window size.



3. Congestion Detection Phase

When sender detects the loss of segments, it reacts in different ways depending on how the loss is detected-

Case-01: Detection On Time Out

- Time Out Timer expires before receiving the acknowledgment for a segment.
- This case suggests the stronger possibility of congestion in the network.
- There are chances that a segment has been dropped in the network.

Reaction

In this case, sender reacts by-

- Setting the slow start threshold to half of the current congestion window size.
- Decreasing the congestion window size to 1 MSS.
- Resuming the slow start phase.

Case-02: Detection On Receiving 3 Duplicate Acknowledgments-

- Sender receives 3 duplicate acknowledge-ments for a segment.
- This case suggests the weaker possibility of congestion in the network.
- There are chances that a segment has been dropped but few segments sent later may have reached.

Reaction

In this case, sender reacts by-

- Setting the slow start threshold to half of the current congestion window size.
- Decreasing the congestion window size to slow start threshold.
- Resuming the congestion avoidance phase.

Short Question and Answers

1. Address space.

Ans :

Address space is the amount of memory allocated for all possible addresses for a computa-tional entity for example, a device, a file, a server or a networked computer. The system provides each device and process address space that holds a specific portion of the processor's address space. This can include either physical or virtual addresses accessible to a processor or reserved for a particular process.

The width of its address bus and registers often restricts the processor's address space. However, a memory management technique called virtual memory can increase the size of the address space to be higher than that of the physical memory.

2. IPv4.

Ans :

Slash notation is a compact way to show or write an IPv4 subnet mask. When you use slash notation, you write the IP address, a forward slash (/), and the subnet mask number.

To find the subnet mask number:

1. Convert the decimal representation of the subnet mask to a binary representation.
2. Count each "1" in the subnet mask. The total is the subnet mask number.

3. Write about classless addressing.

Ans :

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses. In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22 ,..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.

4. What is Network Address Translation? Explain.

Ans :

NAT (Network Address Translation) connects two networks and maps the private (inside local) addresses into public addresses (inside global). Inside local denotes that the best address belonged to an internal network and was not assigned by a Network Information Centre or service power. The inside global signifies that the address is a valid address assigned by the NIC or service provider, and one or more inside local addresses to the outside world.

5. Advantages of NAT.

Ans :

The following are the advantages of NAT:

- NAT protects the public addresses that have been registered and slow down the IP address space exhaustion.
- Removes the address renumbering process that occurs when switching networks
- The occurrence of address overlap was significantly reduced.
- Increases flexibility of the connection establishment.

6. Datagram network.

Ans :

In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.

In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first come, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed.

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multi packet transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.

7. What is Fragmentation in Networking? Explain.

Ans :

IP fragmentation is a process that divides packets into smaller pieces (fragments) so that the resulting pieces can travel across a link with a smaller maximum transmission unit (MTU) than the original packet size. The receiving host reassembles the fragments.

8. What is Checksum? How to apply check-sum for error detection? Explain.

Ans :

The checksum is a network method to check for any error or damage to the data transmitted to the sender side from the sender side. The checksum method applies the bit addition and bit complement method to perform the checksum implementation.

The need to apply checksum or any other error-detection method is done simply to identify the damage to the data when it's being transmitted over the network channel.

The checksum uses the Checksum Generator on the sender side and the Checksum Checker on the receiver side.

9. IPV6.

Ans :

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is a positional number system that uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

10. ICMP Protocol.

Ans :

The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information. For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

11. IGMP.

Ans :

IGMP is an abbreviated form of Internet Group Management Protocol(IGMP). Mainly the Internet Protocol can be involved in the two types of communication i.e, Unicasting and multicasting. IGMP is one of the necessary but not the efficient protocol that is involved in Multicasting.

IGMP is basically a companion of Internet Protocol (IP).

IGMP is not a multicasting routing protocol but it is a protocol that manages the group membership. This protocol mainly helps the multicast routers in order to create and update a list of loyal members that are related to each router interface.

This protocol is used in streaming videos, gaming, or web conferencing tools.

12. What is ARP.

Ans :

Address Resolution Protocol (ARP) is an important protocol of the network layer in the OSI model, which helps find the MAC (Media Access Control) address given the system's IP address. The ARP's main task is to convert the 32-bit IP address (for IPv4) to a 48-bit MAC address.

This protocol is mostly used to determine the hardware (MAC) address of a device from an IP address. It is also used when one device wants to communicate with some other device on a local network. The full form of ARP is Address Resolution Protocol.

13. Reverse Address Resolution Protocol.

Ans :

RARP is abbreviation of Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

This protocol is used to communicate data between two points in a server. The client doesn't necessarily need prior knowledge the server identities capable of serving its request. Media Access Control (MAC) addresses requires individual configuration on the servers done by an administrator. RARP limits to the serving of IP addresses only.

When a replacement machine is set up, the machine may or might not have an attached disk that may permanently store the IP Address so the RARP client program requests IP Address from the RARP server on the router.

Choose the Correct Answers

1. Which of the following does not have a Net ID and Host ID? [d]

   (a) Class A (b) Class B

   (c) Class C (d) Class D

2. The slash notation in classless addressing is referred to as – [c]

   (a) NIFT (b) PITF

   (c) CIDR (d) TRS

3. Which Class is reserved for future use? [d]

   (a) A (b) B

   (c) D (d) E

4. The maximum number of networks that can use Class C addresses in the IPv4 addressing format is _________. [c]

   (a) 2^{14} (b) 2^{7}

   (c) 2^{21} (d) 2^{24}

5. In IPv4, what is needed to determine the number of the last byte of a fragment? [d]

   (a) Identification number (b) Offset number

   (c) Total length (d) ((b) and ((c) D

6. Which of the following is a necessary part of IPv6 diagram [a]

   (a) Base header (b) Extension header

   (c) Data packet from the upper layer (d) ((a) and ((c)

7. Among the following which protocol can be used to report these errors and to debug those errors. [d]

   (a) ARP (b) RARP ICMP

   (c) IGMP (d) ICMP

8. Which type of ARP request helps the network to identify the duplicate IP address [b]

   (a) Proxy ARP (b) Gratuitous ARP

   (c) Reverse ARP (d) Inverse ARP

9. Among the following which protocol is used for dynamic multicasting [c]

   (a) ARP (b) RARP ICMP

   (c) IGMP (d) ICMP

10. _______ is an important protocol of the network layer in the OSI model, which helps find the MAC (Media Access Control) address given the system's IP address. [c]

    (a) ARP (b) RARP ICMP

    (c) IGMP (d) ICMP

Fill in the Blanks

1. ________ connects two networks and maps the private (inside local) addresses into public addresses (inside global).
2. ________ is a process that divides packets into smaller pieces so that the resulting pieces can travel across a link with a smaller maximum transmission unit (MTU) than the original packet size
3. In a ________ network, each packet is treated independently of all others. Even if a packet is part of a multi packet transmission.
4. The header of IPv6 is of fix length of ________ bytes
5. ________ is a tool that tracks the route taken by a packet on an IP network from source to destination.
6. Association between a protocol address and a hardware address is known as ________
7. RARP full form ________
8. In ________ queuing method, the first packet that arrives at a router is the first packet to be transmitted
9. So in a ________ algorithm in which gateways maintain separate queues for packets from each individual source and serviced them in a round-robin manner.
10. TCP reacts to ________ by reducing the sender window size.

Answers

1. NAT (Network Address Translation)
2. Fragmentation
3. Datagram
4. 40
5. Traceroute
6. Binding.
7. Reverse Address Resolution Protocol
8. FIFO
9. Fair queuing
10. Ccongestion

UNIT IV

Congestion Control, Congestion-Avoidance Mechanisms and Quality of Service, Internetworking:

Intra-Domain and Inter-Domain Routings, Unicast Routing Protocols: RIP, OSPF and BGP, Multicast Routing Protocols: DVMRP, PIM-DM, PIM-SM, CBT, MSDP and MOSPF, Spanning Tree Algorithm

4.1 Congestion Control

4.1.1 Congestion-Avoidance Mechanisms And Quality Of Service

Q1. What is congestion control? Explain the principles and techniques of congestion control.

Ans : **(Imp.)**

Meaning

Congestion Control is a type of network layer issue, and it is concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, and there are no lost packets.

Causes

The main cause of congestion is a huge amount of data traffic. But other factors are equally important for making congestion as given below:

1. Sudden arrival of large data (called burst data) from many input lines and trying to access a single output line of a router. In this case, the particular output line is blocked if its bandwidth isn't sufficiently high.
2. Low bandwidth line will produce congestion even if the data rate isn't too high.
3. Mismatch between the speeds of different components of the system may also produce congestion.

Principle

The principles of congestion control are a set of guidelines and techniques that are used to manage network congestion and ensure that the network operates efficiently and effectively. Some of the key principles of congestion control include:

1. **Monitoring network traffic**

   Network congestion can occur when there is more traffic on the network than the network can handle. Therefore, it is essential to monitor network traffic continuously to detect congestion before it becomes a problem.

2. **Feedback-based mechanisms**

   Feedback-based mechanisms are used to control the rate of traffic flow and prevent congestion. These mechanisms involve sending feedback messages to the source of the traffic, indicating the current network conditions and the need to reduce the rate of traffic.

3. **Resource allocation**

   Congestion control involves allocating network resources, such as bandwidth and buffer space, effectively. This ensures that each flow of traffic receives a fair share of network resources and prevents any one flow from monopolizing the network.

4. **Congestion avoidance**

   Congestion avoidance techniques are used to prevent congestion from occurring in the first place. These techniques involve detecting and reacting to early signs of congestion, such as packet loss or delay, and reducing the rate of traffic to prevent congestion from occurring.

5. **Traffic prioritization**

   Congestion control involves prioritizing traffic based on its importance and criticality. This ensures that critical traffic, such as voice or video traffic, is given priority over less critical traffic, such as file downloads.

Techniques

There are several congestion control techniques that can be used to manage network traffic and prevent congestion. Some of the most common techniques include:

1. **Traffic shaping**

   Traffic shaping is a technique that involves regulating the rate of traffic entering the network to ensure that it does not exceed the capacity of the network. This technique can be used to prioritize critical traffic or to limit the amount of non-critical traffic.

2. **Packet dropping**

   Packet dropping is a technique that involves dropping packets when the network becomes congested. This technique can be used to prevent network overload and ensure that critical traffic receives priority.

3. **Resource reservation**

   Resource reservation is a technique that involves reserving network resources, such as bandwidth or buffer space, for specific types of traffic. This technique can be used to ensure that critical traffic receives the necessary resources and priority.

4. **Quality of Service (QoS)**

   QoS is a technique that involves assigning different levels of priority to different types of traffic. This technique can be used to ensure that critical traffic, such as voice or video traffic, receives priority over less critical traffic, such as email or file downloads.

5. **Active Queue Management (AQM)**

   AQM is a technique that involves monitoring the length of network queues and dropping packets before the queue becomes congested. This technique can be used to prevent buffer overflow and ensure that critical traffic receives priority.

6. **Explicit Congestion Notification (ECN)**

   ECN is a technique that involves marking packets when congestion is detected. This technique can be used to signal congestion to end hosts and prevent network overload.

Q2. What are Congestion Avoidance Mechanisms ? Explain.

Ans :

Meaning

Congestion avoidance mechanisms are techniques used to prevent or mitigate network congestion, which occurs when the demand for network resources exceeds the available capacity. congestion avoidance mechanisms are critical to the performance and reliability of computer networks. By preventing or mitigating congestion, these techniques ensure that network traffic flows smoothly and efficiently, which is essential for businesses and organizations that rely on their networks for communication and data transfer.

Here are some common congestion avoidance mechanisms used in computer networks:

1. **Traffic Shaping**

   Traffic shaping is a technique that regulates the flow of network traffic by smoothing out bursts of traffic and ensuring that traffic flows within defined limits. It works by controlling the rate at which traffic is sent and received, which helps prevent congestion by preventing traffic from overwhelming network resources. Traffic shaping can be implemented using various techniques such as leaky bucket, token bucket, or rate limiting.

2. **Quality of Service (QoS)**

   QoS is a mechanism that prioritizes network traffic based on its importance or type. By prioritizing traffic, QoS can ensure that important traffic, such as VoIP or video traffic, is given priority over less important traffic, such as email or file transfers. QoS can be implemented using various techniques such as packet classification, marking, and policing.

3. **Random Early Detection (RED)**

   RED is a technique used to prevent congestion by selectively dropping packets before congestion occurs. RED randomly drops packets when the average queue length exceeds a certain threshold, which helps prevent congestion by allowing congestion to be detected and controlled before it becomes severe. RED is typically used in routers to prevent buffer overflow.

4. Explicit Congestion Notification (ECN)

ECN is a technique used to inform network devices of congestion before it occurs. ECN-capable devices can mark packets to indicate congestion, which allows downstream devices to respond appropriately by reducing the amount of traffic they send. ECN is implemented in routers and hosts and is enabled by default in most modern operating systems.

5. Adaptive TCP

Adaptive TCP is a technique that dynamically adjusts the transmission rate of TCP connections based on network conditions. By adjusting the transmission rate, adaptive TCP can help prevent congestion by preventing TCP connections from overwhelming network resources. Adaptive TCP uses various techniques such as slow start, congestion avoidance, and fast retransmit to adjust the transmission rate.

4.2 Internet working

4.2.1 Intra-Domain And Inter-domain Routings

Q3. What is Routing? Explain Intra- Domain And Inter-domain Routings.

Ans :

Meaning

Routing is the process of directing network traffic from its source to its destination across a network. It is a fundamental concept in computer networking that enables devices on a network to communicate with each other by forwarding packets of data between them. The routing process involves the use of routing protocols and algorithms that determine the optimal path for data to travel from the source to the destination based on various factors, such as network topology, available bandwidth, and network congestion.

Routing can occur at different layers of the networking stack, including the physical layer, data link layer, network layer, and transport layer. At the network layer, routing is typically performed by devices such as routers, which use routing tables and algorithms to determine the best path for data to travel between networks.

In computer networking, intra-domain routing and inter-domain routing are two distinct routing protocols that are used to direct traffic within and between different autonomous systems (AS).

1. Intra-domain routing

Intra-domain routing protocols are used to direct traffic within a single autonomous system (AS). An autonomous system is a collection of networks that are controlled by a single entity or organization. Intra-domain routing protocols are typically used within an organization's network and are designed to ensure that traffic is directed along the most efficient path from the source to the destination within the same AS. Examples of intra-domain routing protocols include OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System).

2. Inter-domain routing

Inter-domain routing protocols are used to direct traffic between different autonomous systems. Inter-domain routing protocols are designed to ensure that traffic is directed along the most efficient path between different autonomous systems, taking into account factors such as network topology, available bandwidth, and cost. Examples of inter-domain routing protocols include BGP (Border Gateway Protocol) and EGP (Exterior Gateway Protocol).

Q4. Write the differences between Inter domain and Intradomain Routing.

Ans : **(Imp.)**

The following table highlights the major differences between interdomain and intradomain routing protocols.

S.No	Intradomain Routing	Interdomain Routing
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.
3.	Protocols used in intradomain routing are known as Interior-gate way protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.
4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.
5.	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).
6.	Some Popular Protocols of this routing are RIP(resource information protocol) and OSPF(open shortest path first).	Popular Protocols of this routing is BGP (Border Gateway Protocol) used to connect two or more AS(autonomous system).

4.3 Unicast Routing Protocols

4.3.1 RIP

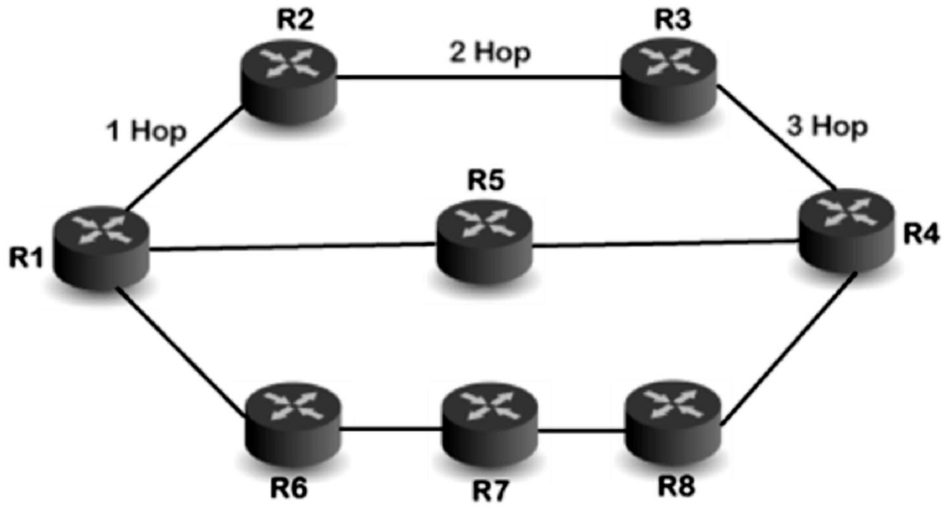
Q5. Explain bout RIP protocol.

Ans :

RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing tables.

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

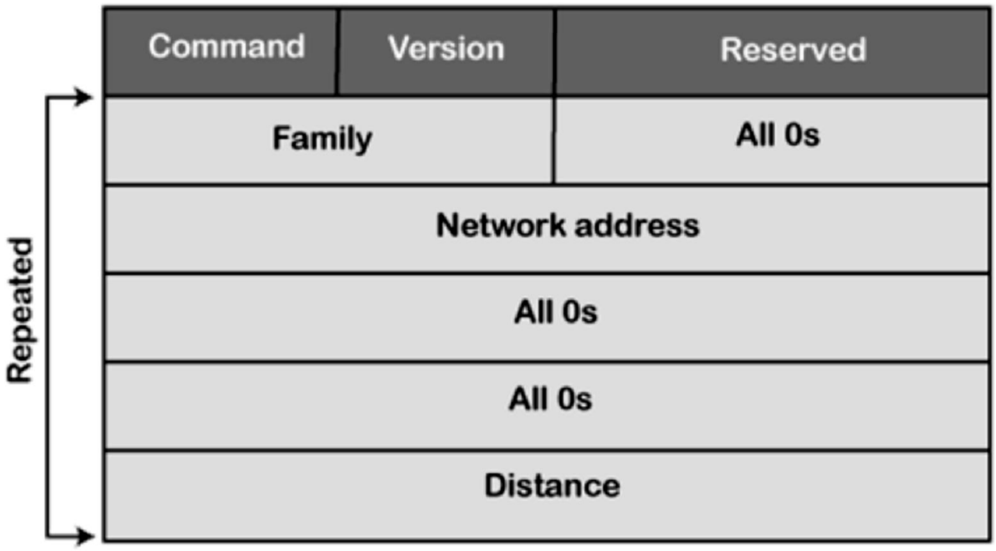
When the router sends the packet to the network segment, then it is counted as a single hop.



In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

RIP Message Format

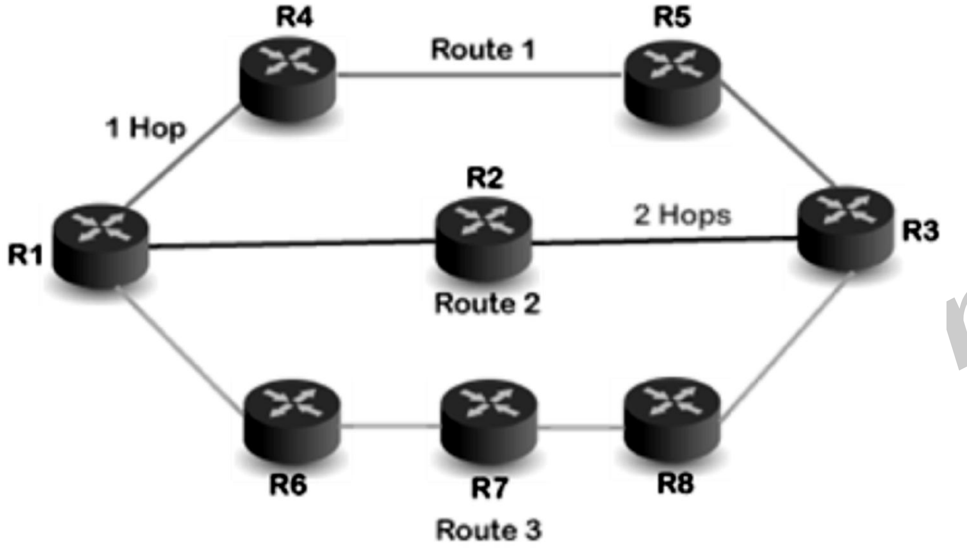
Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



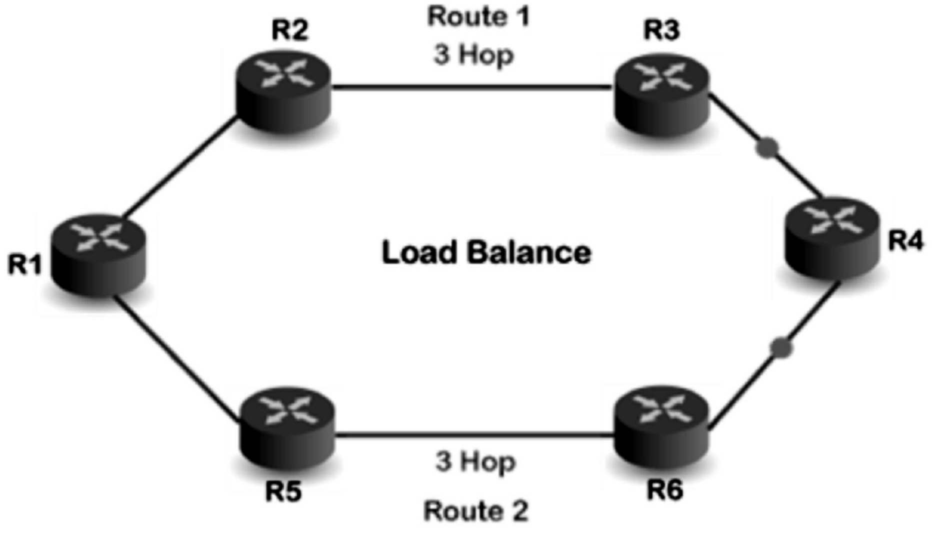
Command	Version	Reserved
Family		All 0s
Network address		
All 0s		
All 0s		
Distance		

- **Command:** It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
- **Version:** Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.

- **Reserved:** This is a reserved field, so it is filled with zeroes.
- **Family:** It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- **Network Address:** It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- **Distance:** The distance field specifies the hop count, i.e., the number of hops used to reach the destination.



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.



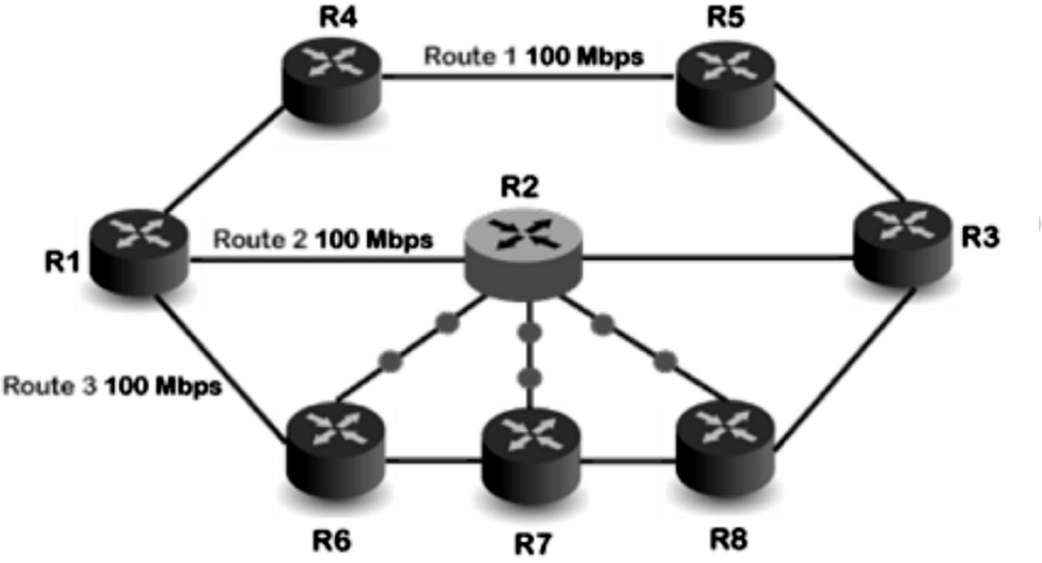
Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

Q6. Explain the Disadvantages of RIP.

Ans :

The following are the disadvantages of RIP:

(a) In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

- The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
- It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
- It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
- The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
- The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

The following timers are used to update the routing table:

- **RIP update timer : 30 sec**

  The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

- **RIP Invalid timer : 180 sec**

  The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

- **RIP Flush timer : 240 sec**

  The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

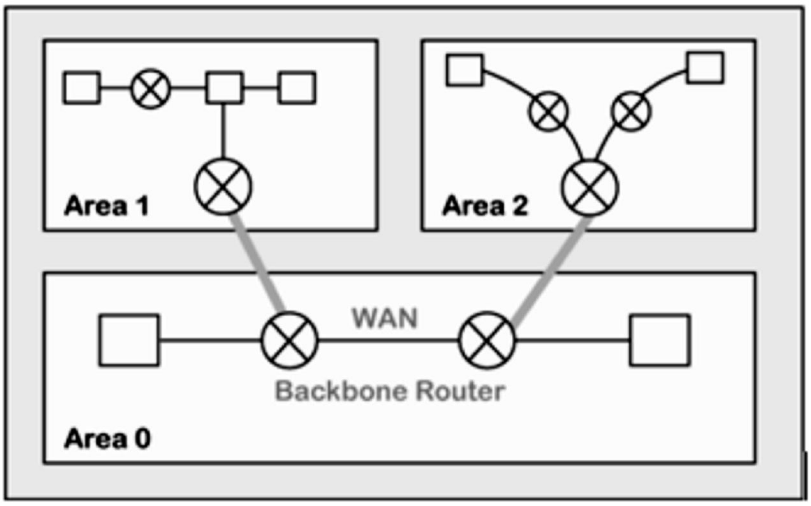
4.3.2 OSPF

Q7. Explain OSPF protocol.

Ans :

The OSPF stands for Open Shortest Path First. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.

OSPF Areas



OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different autonomous system for easy management and OSPF further divides the autonomous systems into Areas.

Routers that exist inside the area flood the area with routing information

In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area. The role of a primary area is to provide communication between different areas.

Working

There are three steps that can explain the working of OSPF:

Step 1:

The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2:

The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3:

The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

Router forms a neighbor relationship

The first thing is happened before the relationship is formed is that each router chooses the router ID.

Router ID (RID): The router ID is a number that uniquely identifies each router on a network. The router ID is in the format of the IPv4 address. There are few ways to set the router ID, the first way is to set the router ID manually and the other way is to let the router decides itself.

The following is the logic that the router chooses to set the router ID:

➢ **Manually assigned**

The router checks whether the router ID is manually set or not. If it manually set, then it is a router ID. If it is not manually set, then it will choose the highest 'up' status loopback interface IP address. If there are no loopback interfaces, then it will choose the highest 'up' status non-loopback interface IP address.

Two routers connected to each other through point to point or multiple routers are connected can communicate with each other through an OSPF protocol. The two routers are adjacent only when both the routers send the HELLO packet to each other. When both the routers receive the acknowledgment of the HELLO packet, then they come in a two-way state. As OSPF is a link state routing protocol, so it allows to create the neighbor relationship between the routers. The two routers can be neighbors only when they belong to the same subnet, share the same area id, subnet mask, timers, and authentication. The OSPF relationship is a relationship formed between the routers so that they can know each other. The two routers can be neighbors if atleast one of them is designated router or backup designated router in a network, or connected through a point-to-point link.

Types

A link is basically a connection, so the connection between two routers is known as a link.

There are four types of links in OSPF:

1. **Point-to-point link**

   The point-to-point link directly connects the two routers without any host or router in between.

2. **Transient link**

   When several routers are attached in a network, they are known as a transient link.

   The transient link has two different imple mentations:

Unrealistic topology

When all the routers are connected to each other, it is known as an unrealistic topology.

Realistic topology

When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.

3. **Stub link**

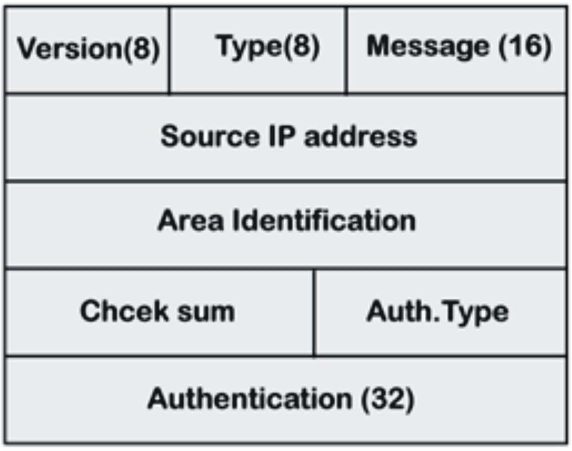
It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.

4. **Virtual link**

If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

OSPF Message Format

The following are the fields in an OSPF message format:



<table>
<tr><td>Version(8)</td><td>Type(8)</td><td>Message (16)</td></tr>
<tr><td colspan="3">Source IP address</td></tr>
<tr><td colspan="3">Area Identification</td></tr>
<tr><td colspan="2">Chcek sum</td><td>Auth.Type</td></tr>
<tr><td colspan="3">Authentication (32)</td></tr>
</table>

- **Version**

  It is an 8-bit field that specifies the OSPF protocol version.

- **Type**

  It is an 8-bit field. It specifies the type of the OSPF packet.

- **Message**

  It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.

- **Source IP address**

  It defines the address from which the packets are sent. It is a sending routing IP address.

- **Area identification**

  It defines the area within which the routing takes place.

- **Checksum**

  It is used for error correction and error detection.

- **Authentication type**

  There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.

- **Authentication**

  It is a 32-bit field that contains the actual value of the authentication data.

Q8. Explain about OSPF Packets.

Ans :

There are five different types of packets in OSPF:

1. **Hello packet**

The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.

2. **Database Description**

After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.

3. **Link state request**

The link-state request is sent by the router to obtain the information of a specified route.

Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.

4. **Link state update**

The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.

5. **Link state acknowledgment**

The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

Q9. Explain about OSPF States.

Ans :

The device running the OSPF protocol undergoes the following states:

- **Down**

  If the device is in a down state, it has not received the HELLO packet. Here, down does not mean that the device is physically down; it means that the OSPF process has not been started yet.

- **Init**

  If the device comes in an init state, it means that the device has received the HELLO packet from the other router.

- **2WAY**

  If the device is in a 2WAY state, which means that both the routers have received the HELLO packet from the other router, and the connection gets established between the routers.

- **Exstart**

  Once the exchange between the routers get started, both the routers move to the Exstart state. In this state, master and slave are selected based on the router's id. The master controls the sequence of numbers, and starts the exchange process.

- **Exchange**

  In the exchange state, both the routers send a list of LSAs to each other that contain a database description.

- **Loading**

  On the loading state, the LSR, LSU, and LSA are exchanged.

- **Full**

  Once the exchange of the LSAs is completed, the routers move to the full state.

Q10. Explain about Router attributes.

Ans :

Before going to the Extract state, OSPF chooses one router as a Designated router and another router as a backup designated router. These routers are not the type, but they are the attributes of a router. In the case of broadcast networks, the router selects one router as a designated router and another router as a backup designated router. The election of designated and the backup designated router is done to avoid the flooding in a network and to minimize the number of adjacencies. They serve as a central point for exchanging the routing information among all the routers. Since point-to-point links are directly connected, so DR and BDR are not elected.

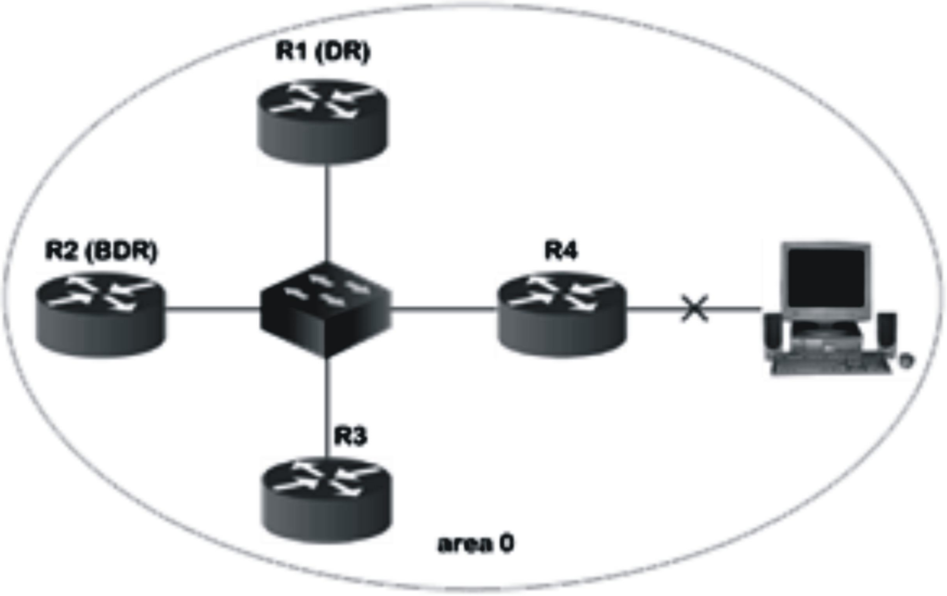
If DR and BDR are not elected, the router will send the update to all the adjacent neighbors, leading to the flooding in a network. To avoid this problem, DR and BDR are elected. Each non-DR and non-BDR send the update only to the DR and BDR instead of exchanging it with other routers in a network segment. DR then distributes the network topology information to other routers in the same area whereas the BDR serves a substitute for the DR. The BDR also receives the routing information from all the router but it does not distribute the information. It distributes the information only when the DR fails.

The multicast address 224.0.0.6 is used by the non-DR and non-BDR to send the routing information to the DR and BDR. The DR and BDR send the routing information to the multicast address 224.0.0.5.

Based on the following rules, the DR and BDR are elected:

- The router with the highest OSPF priority is chosen as the DR. By default, the highest priority is set as 1.
- If there is no highest priority, then the router with the highest router Id is chosen as the DR, and the router with the second-highest priority is chosen as the BDR.

Let's understand this scenario through an example.



In the above figure, R1 is chosen as the DR, while R2 is chosen as the BDR as R1 has the highest router ID, whereas the R2 has the second-highest router ID. If the link fails between R4 and the system, then R4 updates only R1 and R4 about its link failure. Then, DR updates all the non-DR and non-BDR about the change, and in this case, except R4, only R3 is available as a non-DR and non-BDR.

4.3.3 BGP

Q11. Explain BGP protocol.

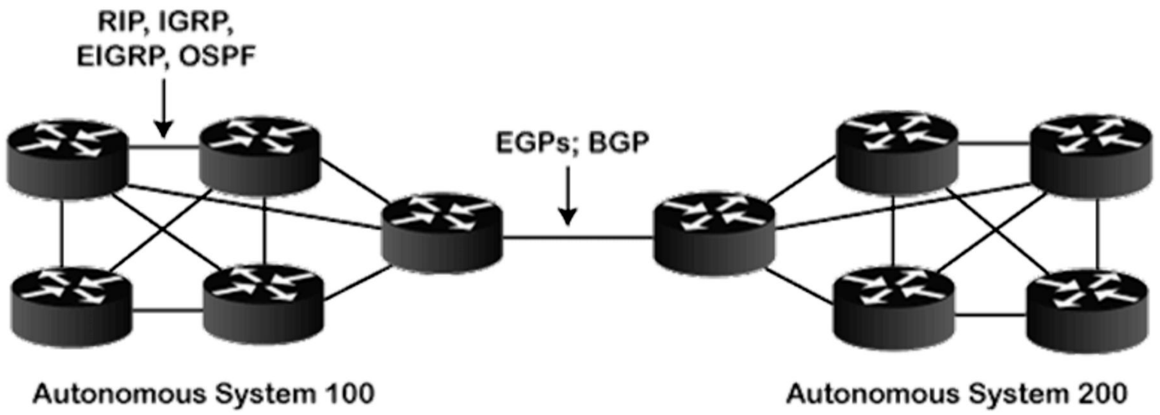
Ans :

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

There are many versions of BGP, such as:

- BGP version 1: This version was released in 1989 and is defined in RFC 1105.
- BGP version 2: It was defined in RFC 1163.
- BGP version 3: It was defined in RFC 1267.
- BGP version 4: It is the current version of BGP defined in RFC 1771.

BGP Autonomous Systems



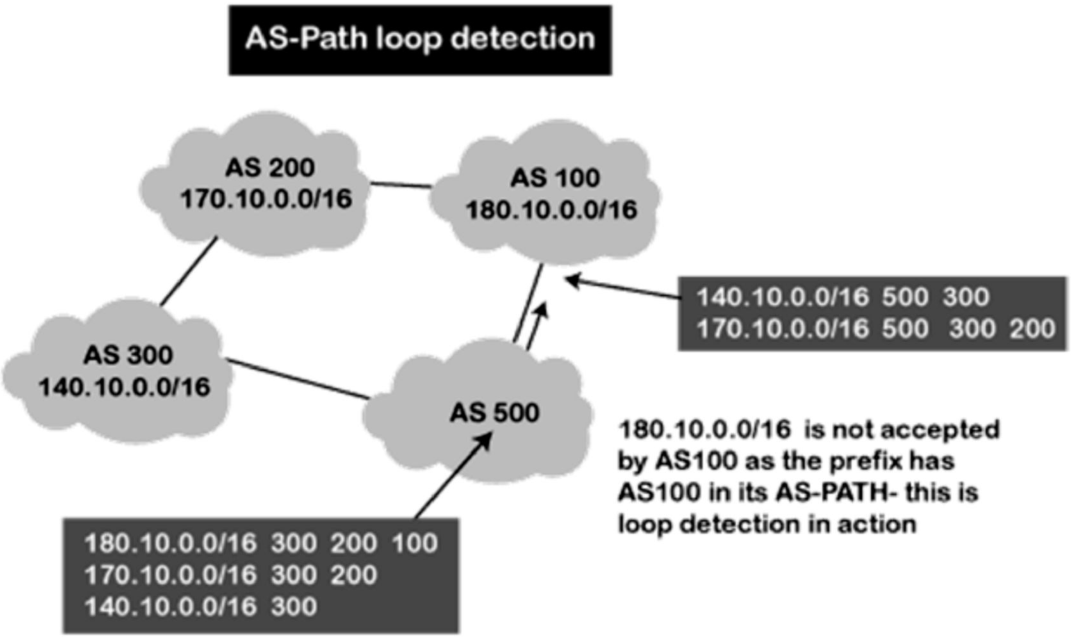
An autonomous system is a collection of networks that comes under the single common administrative domain. Or we can say that it is a collection of routers under the single administrative domain.

For example, an organization can contain multiple routers having different locations, but the single autonomous number system will recognize them. Within the same autonomous system or same organization, we generally use IGP (Interior Gateway Protocol) protocols like RIP, IGRP, EIGRP, OSPF. Suppose we want to communicate between two autonomous systems. In that case, we use EGP (Exterior Gateway Protocols). The protocol that is running on the internet or used to communicate between two different autonomous number systems is known as BGP (Border Gateway Protocol). The BGP is the only protocol that is running on the internet backbone or used to exchange the routes between two different autonomous number systems. Internet service providers use the BGP protocol to control all the routing information.

Features

- **Open standard-** It is a standard protocol which can run on any window device.
- **Exterior Gateway Protocol -**It is an exterior gateway protocol that is used to exchange the routing information between two or more autonomous system numbers.
- **Inter AS-domain routing -** It is specially designed for inter-domain routing, where inter AS-domain routing means exchanging the routing information between two or more autonomous number system.
- **Supports internet -** It is the only protocol that operates on the internet backbone.
- **Classless -** It is a classless protocol.
- **Incremental and trigger updates -** Like IGP, BGP also supports incremental and trigger updates.
- **Path vector protocol -** The BGP is a path vector protocol. Here, path vector is a method of sending the routes along with routing information.
- **Configure neighborhood relationship -** It sends updates to configure the neighborhood relationship manually. Application layer protocol

BGP's Loop prevention mechanism

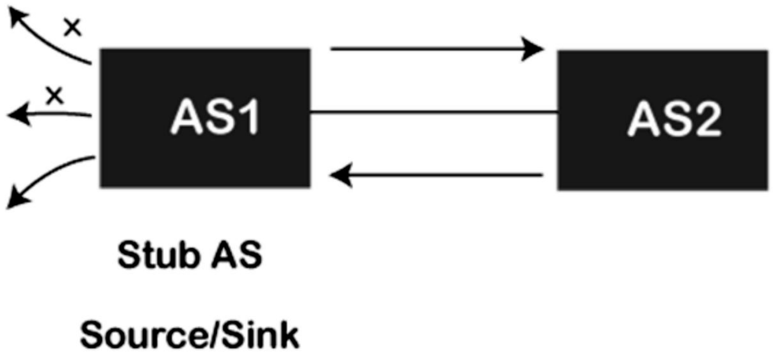


There is a possibility that when you are connecting to the internet, then you may be advertising route 10.0.0.0 to some autonomous system, then it is advertised to some other autonomous system. Then there is a possibility that the same route is coming back again. This creates a loop. But, in BGP, there is a rule that when the router sees its own AS number for example, as shown in the above figure, the network 180.10.0.0/16 is originating from the AS 100, and when it sends to the AS 200, it is going to carry its path information, i.e., 180.10.0.0/16 and AS 100. When AS 200 sends to the AS 300, AS 200 will send its path information 180.10.0.0/16 and AS path is 100 and then 200, which means that the route originates from AS 100, then reaches 200 and finally reaches to 300. When AS 300 sends to the AS 500, it will send the network information 180.10.0.0/16, and AS path is 100, 200, and then 300. If AS 500 sends to the AS 100, and AS 100 sees its own autonomous number inside the update, it will not accept it. In this way, BGP prevents the loop creation.

Types of Autonomous systems

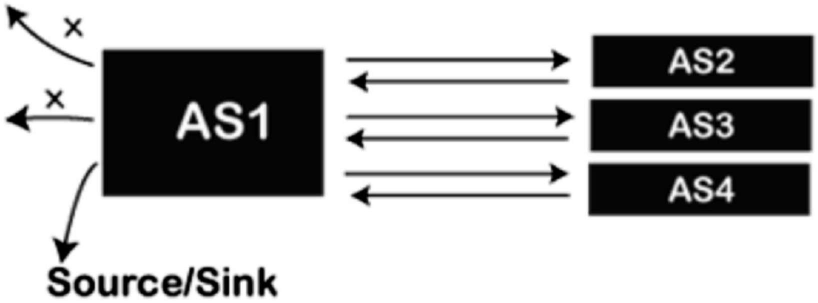
The following are the types of autonomous systems:

➢ Stub autonomous system



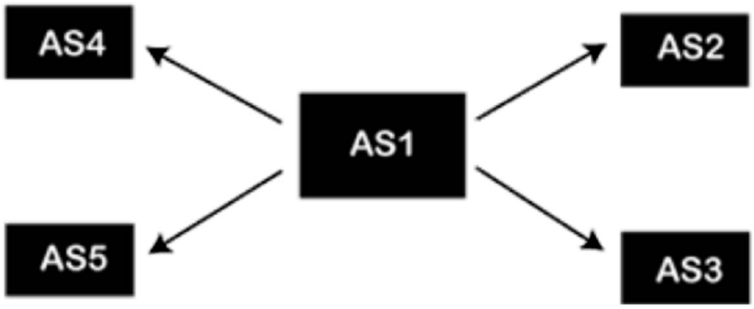
It is a system that contains only one connection from one autonomous system to another autonomous system. The data traffic cannot be passed through the stub autonomous system. The Stub AS can be either a source or a sink. If we have one autonomous system, i.e., AS1, then it will have a single connection to another autonomous system, AS2. The AS1 can act either as a source or a sink. If it acts as a source, then the data moves from AS1 to AS2. If AS1 acts as a sink, means that the data gets consumed in AS1 which is coming from AS2, but the data will not move forward from AS1.

➢ Multihomed autonomous system



It is an autonomous system that can have more than one connection to another autonomous system, but it can still be either a source or a sink for data traffic. There is no transient data traffic flow, which means that the data can be passed from one autonomous system.

➢ Transient Autonomous System

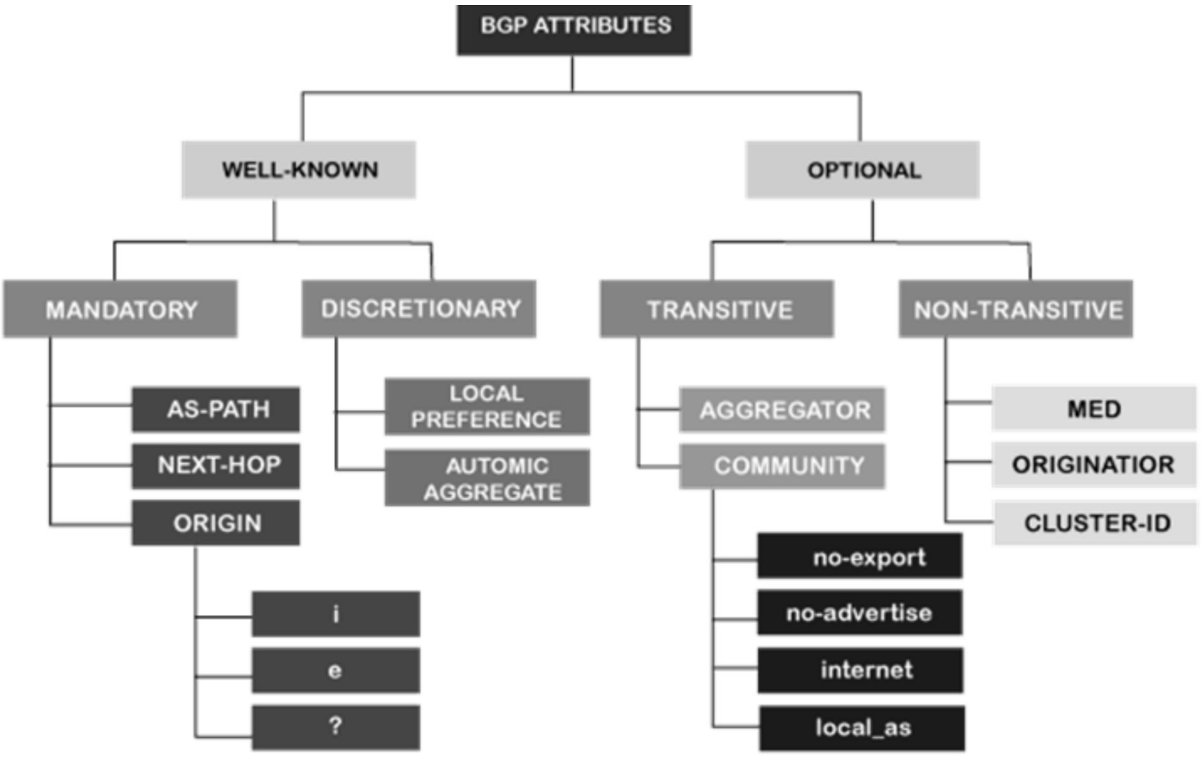


The transient autonomous system is a multihomed autonomous system, but it also provides transient traffic flow.

Path attributes

The BGP chooses the best route based on the attributes of the path.

As we know that path-vector routing is used in the border gateway routing protocol, which contains the routing table that shows the path information. The path attributes provide the path information. The attributes that show or store the path information are known as path attributes. This list of attributes helps the receiving router to make a better decision while applying any policy. Let's see the different types of attributes. The path attribute is broadly classified into two categories:



1. **Well-known attribute :** It is an attribute that should be recognized by every BGP router.

   The well-known attribute is further classified into two categories:

- **Well-known mandatory :** When BGP is going to advertise any network, but it also advertises extra information, and that information with path attributes information. The information includes AS path information, origin information, next-hop information. Here, mandatory means that it has to be present in all the BGP routing updates.
- **Well-known discretionary :** It is recognized by all the BGP routers and passed on to other BGP routers, but it is not mandatory to be present in an update.

2. **Optional attribute :** It is an attribute that is not necessarily to be recognized by every BGP router. In short, we can say that it is not a mandatory attribute.

   The optional attribute is further classified into two categories:

- **Optional transitive:** BGP may or may not recognize this attribute, but it is passed on to the other BGP neighbors. Here, transitive means that if the attribute is not recognized, then it is marked as a partial.
- **Optional non-transitive:** If the BGP cannot recognize the attribute, it ignores the update and does not advertise to another BGP router.

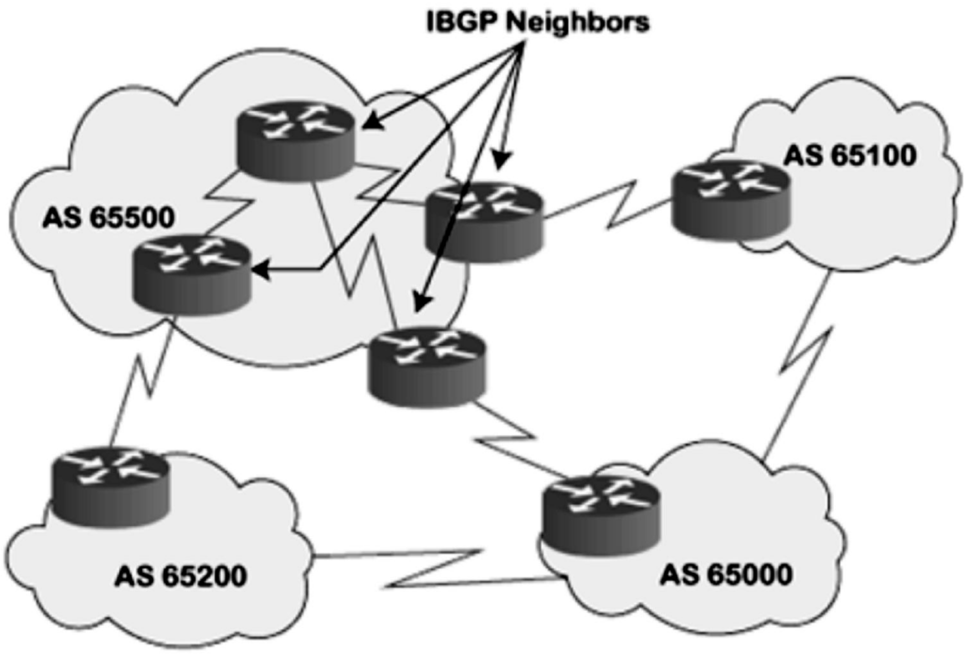
BGP Neighbors

BGP neighborship is similar to the OSPF neighborship, but there are few differences. BGP forms the neighboring relationship with the help of the TCP connection on port number 179 and then exchanges the BGP updates. They exchange the updates after forming the neighbor relationship. In BGP, the neighbor relationship is configured manually. BGP neighbors are also known as BGP peers or BGP speakers.

There are two types of neighbor relationship:

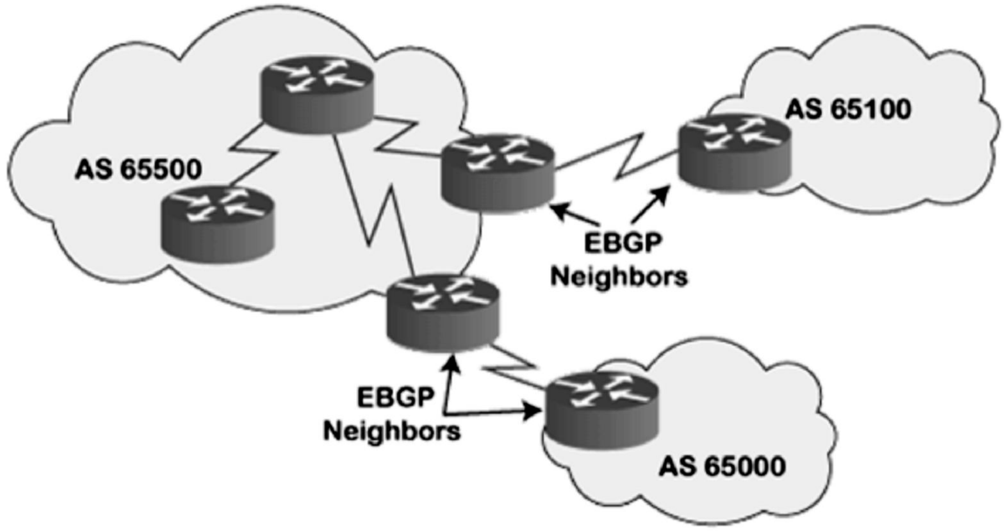
- **IBGP (Internal BGP):** If all the routers are neighbors of each other and belong to the same autonomous number system, the routers are referred to as an IBGP.

IBGP neighbors



- **EBGP (External BGP):** If all the routers are neighbors of each other and they belong to the different autonomous number systems, then the routers are referred to as an EBGP.

EBGP neighbors



BGP Tables

There are three types of BGP tables:

- **Neighbor table:** It contains the neighbors who are configured by the administrator manually. The neighbor relationship has to be manually configured by using the neighbor command.
- **BGP forwarding table:** It contains all the routes advertised in BGP and can be verified using the following command:
- **IP routing table:** The IP routing table contains the best path routes required to reach the destination. The following command shows the best routing path:

BGP Sessions

When we talk about the BGP, which means that the communication between the autonomous systems. Let's consider two autonomous systems having five nodes each.

BGP sessions are classified into two categories:

1. **Internal BGP session**

   The internal BGP session is used to exchange information between the routers inside an autonomous system. In short, we can say that the routing information is exchanged between the routers of the same autonomous system.

2. **External BGP session**

   The external BGP session is a session in which nodes or routers of different autonomous systems communicate with each other.

Types of packets

There are four different types of packets exist in BGP:

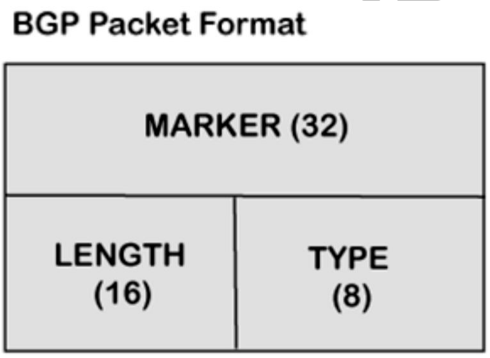
- **Open:** When the router wants to create a neighborhood relation with another router, it sends the Open packet.
- **Update:** The update packet can be used in either of the two cases:

1. It can be used to withdraw the destination, which has been advertised previously.
2. It can also be used to announce the route to the new destination.

- **Keep Alive:** The keep alive packet is exchanged regularly to tell other routers whether they are alive or not. For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.
- **Notification:** The notification packet is sent when the router detects the error condition or close the connection.

BGP Packet Format

Now we will see the format in which the packet travels. The following are the fields in a BGP packet format:



1. **Marker:** It is a 32-bit field which is used for the authentication purpose.
2. **Length:** It is a 16-bit field that defines the total length of the message, including the header.
3. **Type:** It is an 8-bit field that defines the type of the packet.

4.4 Multicast Routing Protocols

4.4.1 DVMRP

Q12. Explain Distance Vector Multicast Routing Protocol.

Ans :

The distance vector multicast routing protocol is multicast routing protocol that takes the routing decision based upon the source address of the packet.

- This algorithm constructs the routing tree for a network.
- Whenever a router receives a packet, it forwards it to some of its ports based on the source address of packet.

2. It must prevent the formation of duplicate packets.
3. It must ensure that the path traveled by a packet is the shortest from its source to the router.
4. It should provide dynamic membership.

To accomplish this, the DVMR algorithm uses a process based on following decision making strategies:

1. Reverse Path Forwarding (RPF)

- In this strategy, the router only forwards those packets that have traveled the shortest path from source to destination.
- To achieve this, the router pretends that it has a packet to send to the source from where the packet has arrived.
- In this way, the shortest path to the sender of the packet is computed.
- If the same route is followed by the received packet, it is forwarded to the next router and it is discarded otherwise.
- The reverse path forwarding ensures that the network receives a copy of the packet without formation of loops. A loop occurs when a packet that has left the router may come back again from another interface or the same interface and be forwarded again.
- RPF does not guarantee that there would be no duplicate packets in the network i.e. the network may receive two or more copies.
- The reason for this is that the routing is based on the source address and not on the destination address.

2. Reverse Path Broadcasting (RPB)

- In order to solve the problem, RPB is used.
- In this method, one parent router is defined for each network.
- The network could accept the multicast packets from this parent router only.
- This router sends packets to those ports for which it is designated as parent.
- Thus, RPB principle' allows a router to broadcast the packet in the network.

This creates duplicate packets on the network and reduces the network efficiency.

3. Reverse Path Multicasting (RPM)

- To overcome the problem of broadcasting in RPB, Reverse Path Multicasting in used.
- In this the desired multicast network tree is created by using two different methods: Pruning and grafting.
- A router can send a prune message to its upstream router whenever it finds that its network is not interested in a multicast packet. In this way a router prunes (cuts) its network from multicasting.
- If a router receives prune message from all the downstream routers, it in turn, sends a prune message to its upstream router.
- A router can also send a graft message to its upstream router if it finds that its network is again interested in receiving the multicast packet. In this way, graft message forces the upstream router to resume sending the multicast message. The network is again grafted (joined).

4. Multicast Open Shortest Path First (MOSPF)

- Multicast open shortest path first is the multicast version of open shortest path first protocol.
- It is an extension of OSPF that uses multicast link state routing method to create source based trees.
- The method used by MOSPF is different from DVMRP.
- The first difference is· that in this method, the tree is least cost tree instead of shortest path tree.
- The second difference is that the tree is not made gradually. It is made immediately it is prepared and ready to use.

4.4.2 PIM-DM

Q13. What is PIM?

Ans :

Meaning

PIM (Protocol Independent Multicast) is a family of multicast routing protocols that are designed to efficiently distribute multicast traffic across a network. PIM can be used in different modes depending on the network topology and the type of multicast traffic being distributed.

Modes

1. **Dense Mode (PIM-DM)**

   Dense mode is used in networks with high-density multicast traffic where most of the network nodes are interested in the multicast traffic. In PIM-DM, multicast traffic is initially flooded to all network nodes, and then pruned back based on the network topology and multicast group membership.

2. **Sparse Mode (PIM-SM)**

   Sparse mode is used in networks with sparse multicast traffic where only a small subset of nodes are interested in the multicast traffic. In PIM-SM, multicast traffic is forwarded only to those networks that have receivers for that multicast group.

   PIM also has a Bidirectional mode (PIM-BIDIR) that is used in networks where multicast traffic is bidirectional, such as video conferencing.

   PIM is a protocol-independent multicast routing protocol, which means that it can work with different unicast routing protocols, such as OSPF, BGP, or IS-IS. PIM uses different mechanisms to build multicast distribution trees and to forward multicast traffic, such as Reverse Path Forwarding (RPF) and Shared Trees.

Component

The main components of the PIM (Protocol Independent Multicast) protocol are as follows:

1. **Multicast group membership management**

   PIM includes mechanisms to manage multicast group membership and to distribute multicast traffic to interested receivers. PIM can work with different multicast group membership protocols, such as IGMP or MLD.

2. **Multicast routing protocols**

   PIM can work with different unicast routing protocols, such as OSPF or BGP, to exchange routing information and to build multicast distribution trees.

3. **Multicast forwarding mechanisms**

   PIM includes different mechanisms to forward multicast traffic, such as Reverse Path Forwarding (RPF) and Shared Trees. RPF ensures that multicast traffic is forwarded in the direction of the root of the multicast tree and avoids loops. Shared Trees allow multiple multicast groups to share the same distribution tree, reducing the overhead of building separate trees for each group.

4. **Multicast traffic control mechanisms**

   PIM includes mechanisms to control multicast traffic, such as pruning, which removes branches of the multicast tree where there are no receivers. Pruning reduces unnecessary multicast traffic and conserves network resources.

5. **Multicast rendezvous points**

   In PIM-SM, a multicast rendezvous point (RP) is used to bootstrap multicast traffic distribution and to build multicast trees. The RP is a centralized point where multicast traffic is initially sent before being distributed to interested receivers.

Q14. Explain PIM –DM protocol.

Ans :

PIM Dense-Mode

PIM-DM (Protocol Independent Multicast - Dense Mode) is a multicast routing protocol that is used to efficiently distribute multicast traffic in a dense network with high bandwidth connectivity. It is a flood-and-prune protocol, which means that multicast traffic is initially flooded to all connected networks and then pruned back based on the network topology and multicast group membership.

In PIM-DM, multicast traffic is forwarded to all directly connected networks until it reaches a network where there are receivers interested in the traffic. Once a receiver is found, the multicast traffic is forwarded only to those networks that have receivers for that multicast group. PIM-DM builds a multicast distribution tree that is rooted at the source and extends to all receivers.

PIM-DM uses a reverse path forwarding (RPF) algorithm to prevent loops and to ensure that multicast traffic is forwarded in the direction of the root of the multicast tree. PIM-DM also uses a prune mechanism to remove branches of the multicast tree where there are no receivers.

PIM-DM is suitable for networks with high-density multicast traffic and where bandwidth is not an issue. It is less suitable for networks with sparse multicast traffic and limited bandwidth.

Being Built Back to the Sender.

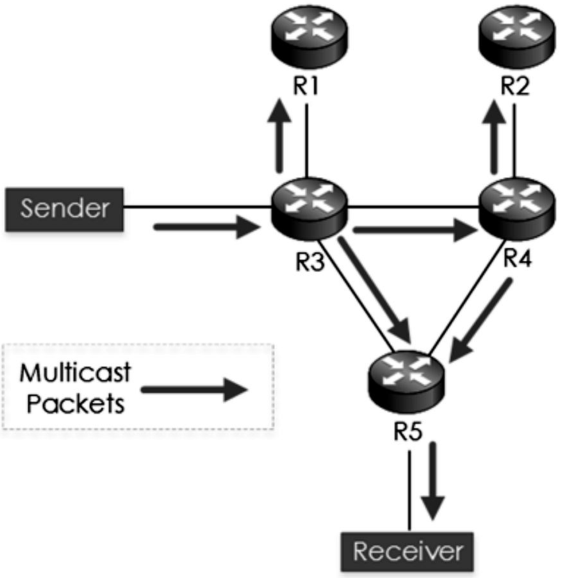


Fig : . PIM-DM Flooding ; (S, G)

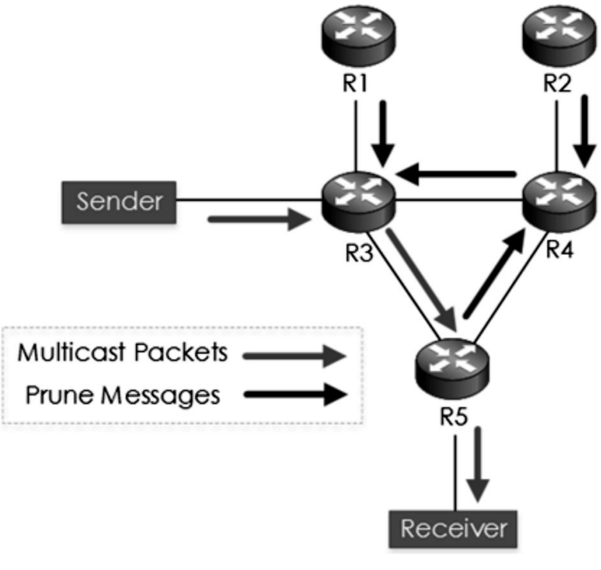


Fig:. PIM-DM Pruning

Working of PIM_DM

Here are the main steps involved in the working of PIM-DM:

1. **Discovery of multicast sources**

   The first step in PIM-DM is the discovery of multicast sources. Multicast sources are identified using multicast group addresses and their associated network interface addresses.

2. **Building the multicast distribution tree**

   PIM-DM builds a multicast distribution tree by flooding multicast traffic to all network nodes. This flood occurs in an expanding ring search manner, which means that the multicast traffic is initially flooded to the directly connected network nodes, and then to progressively more distant nodes.

3. **Pruning the multicast distribution tree**

   After the multicast traffic has been flooded to all network nodes, PIM-DM prunes the multicast distribution tree based on the network topology and multicast group membership. Pruning involves removing branches of the multicast tree where there are no receivers, reducing the amount of multicast traffic on the network.

4. **Maintaining the multicast distribution tree**

   PIM-DM continuously monitors the multicast distribution tree to detect changes in network topology or multicast group membership. If a change is detected, PIM-DM updates the tree accordingly.

5. **Forwarding multicast traffic**

   Once the multicast distribution tree has been built and pruned, PIM-DM forwards multicast traffic to only those network nodes that have requested it. This reduces unnecessary multicast traffic on the network and conserves network resources.

4.4.3 PIM-SM

Q15. Explain PIM-SM protocol.

Ans :

Meaning

PIM-SM works in the opposite manner to PIM-DM; with PIM sparse mode no multicast traffic is forwarded unless some requests it. PIM-SM works via the use of an RP (Rendezvous Point).

Let us look at the process that PIM-SM takes:

1. **Shared Tree (RP to Receiver)**

   The receiver sends an IGMP Join message to the first hop router (FHR), i.e its direct neighboring router. This router will then send a PIM Join to the RP. A shared tree is then built from the receiver to RP based upon (*, G).

2. **Shortest Path Tree (Source to RP)**

   Next, the source starts to send multicast traffic. The FHR encapsulates the multicast packet into a PIM register message and sends via unicast to the RP router. The RP decapsulates the packet and checks the multicast group to see if it has any state for any receivers for the multicast group. If so the RP sends a PIM Join message back towards the source, in order to build an SPT (Shortest Path Tree) back to the source.

   The source sends another multicast packet, however now there is a SPT (aka source tree) from the RP to the FHR. Therefore the packet is now sent across the distribution tree to the RP. The RP receives the packet nativity (with S, G), and in turn, sends a register-stop message back to the sources FHR to stop receiving the register messages (via unicast).

   At this point (Figure 5), we now have a

- source tree from RP to the source,
- shared tree from RP to the receiver.

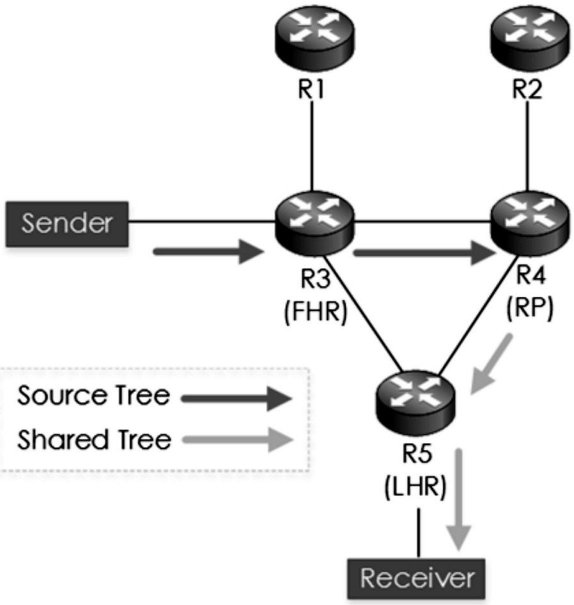


Fig:. PIM Sparse, SPT and Shared Tree

3. Shortest Path Tree Switchover

Although having the RP join back towards the source removes the encapsulation overhead, it does not completely optimize the forwarding paths. As for our receivers, the path via the RP (shared tree) still may be suboptimal. To overcome this, the process to migrate the shared tree to source tree, as known as the SPT switch over begins.

First, the LHR sees the source address of the multicast stream. Now that the LHR knows the source address, it sends an (S, G) Join to the source of the multicast stream. This builds an SPT from LHR to FHR. Finally, a Prune message is sent from the LHR to the RP in order to remove the previously used (RP to LHR) shared tree (Figure 6).

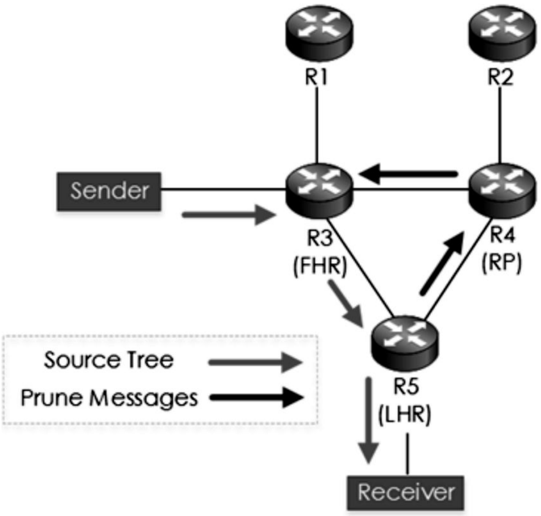


Fig:. SPT Switchover

4.4.4 CBT

Q16. What is CBT ? Explain it.

Ans :

Meaning

The Core-Based Tree (CBT) protocol is a group-shared protocol that uses a core as the root of the tree. The autonomous system is divided into regions, and a core (center router or rendezvous router) is chosen for each region.

There is a core address and a group identifier associated with every group. The core address is the normal unicast address of the core router. This address is used to get packets to the tree. Once on the tree, the packet is multicast based on a globally unique group identifier or group-id.

1) Identification of Core Router

The placement of a group's core should reflect that group's characteristics since the core placement assists in optimizing the routes between any sender and group members on the tree. A router could become a core when a host on one of its attached subnets wishes to initiate a group. Or in case of a single sender, the router nearest to it could become a core. The topic of core placement is open for research.

2) Data Forwarding

Unicast routing is used to route multicast packets to a multicast tree, allowing multicast groups and multicast packets to remain "invisible" to routers not on the tree. This allows for CBT unaware routers in between and is a good strategy for incremental deployment. This is achieved by using the unicast address of the core in the destination field of multicast packets originating off-tree. Data packets destined for a particular group tree carry the group core address in the "destination field" and group-id in the "option" field of IP packet's header.

Once on the corresponding tree (i.e. on arrival at an on-tree router), multicast packets span the tree based on the packet's group-identifier, or group-id.

Core-address in the "destination field" is discarded and group-id in the "option" field is placed in the "destination field". This leads to faster on-tree switching since it is faster to process fixed length header than an extended header. CBT routers forward arriving packets based on the information contained in their CBT Forwarding Information Base.

3) Tree Formation

When a receiver joins a multicast group, its local CBT router looks up the multicast address and obtains the address of the Core router for the group. It then sends a Join-Request message for the group towards the Core. The Join-Request is forwarded to the next-hop router on the path to the core as determined by the unicast forwarding table. The join continues its journey until it either reaches the addressed core, or reaches a CBT capable router that is already part of the tree. At this point, the join's journey is terminated by the receiving router and a Join-Ack is sent. At each CBT router traversed by the Join-Ack, forwarding state is instantiated. In this way, a multicast tree is built.

When a receiver wants to quit a multicast group, same procedure is followed (Quit-Req and Quit-Ack).

Path (or) Node Failure

Link failure is recognizable as a result of "Keep-Alive" mechanism operating between adjacent on-tree routers.

For any non-core router, if a parent or path to parent fails, there are two options

(a) It submits a new Join-Request message, hence keeping the failure transparent to the downstream branch. OR

(b) Tell downstream routers about the failure and allow them to independently attempt to re-attach themselves to the tree.

I. Advantages of Core Based Trees

1) Scalability

Instead of one tree per (source,group) pair as in source based trees, there is one multicast tree per group. So the amount of state that needs to be stored at each router on the tree is O(number of groups) i.e. link information per tree. Moreover, all routers need not support or implement this protocol for this protocol to work i.e. routers which have no members wrt a particular group need not maintain any information as to the existence of that group.

2) **Tree Creation is receiver based**

Only a router interested in becoming a part of the group (or is on the path between a potential member and the tree) is involved in becoming a part of the tree for that particular group. So tree building overhead is restricted to these routers.

3) It is independent of underlying unicast routing algorithm, resulting in a much simplified multicast tree formation across domain boundaries.

II. Disdvantages of Core Based Trees

1) **Core Placement**

Core based trees may not provide the most optimal paths between members of a group.

2) **The Core as a Single Point of Failure**

This problem can be solved by having multiple cores associated with each tree, at the cost of increased complexity.

Two choices with multiple core nodes

(a) **Single Core CBT Trees**

We have multiple "backup" cores to increase the probability that every network node can reach at least one of the cores of a CBT tree. There are multiple cores, which join each other at group initiation time. The primary core is considered the "central-hub" of a tree, with additional nodes simply providing an element of robustness to the design. If the primary core should fail, the recovery scenario is same as that in case of Path or Node Failure. * This has the dynamic Join Overhead.

(b) **Multiple Core CBT Trees**

In this subsets of tree attached to each of core routers. It may lead to optimization of routes between those members. There must be an explicit protocol operating amongst the "backup cores" to handle failure, unlike the earlier case.

4.4.5 MSDP AND MOSPF

Q17. What is MSDP protocol? Explain how to configure it.

Ans : **(Imp.)**

Meaning

MSDP (Multicast Source Discovery Protocol) is a protocol used in multicast networks to distribute information about active multicast sources across multiple Autonomous Systems (ASes). It is used in combination with PIM (Protocol Independent Multicast) to enable multicast traffic to flow between multiple PIM domains.

Components

Here are the main components and features of MSDP:

1. **MSDP Speakers**

MSDP Speakers are routers that participate in MSDP and exchange information about multicast sources with other MSDP Speakers in different PIM domains. MSDP Speakers are usually located at the border of two different PIM domains.

2. **MSDP Peers**

MSDP Peers are MSDP Speakers that have established a peering relationship with each other. They exchange information about active multicast sources using the MSDP protocol.

3. **Multicast Source Active Advertisement (SA) messages**

MSDP uses SA messages to advertise the existence of active multicast sources to other MSDP Peers. SA messages are sent by MSDP Speakers and contain information about the multicast group address, the source address, and the RP (Rendezvous Point) associated with the multicast group.

4. **Rendezvous Point (RP)**

An RP is a designated router that acts as a root for a particular multicast group. MSDP uses RPs to distribute information about active multicast sources to other PIM domains. Each PIM domain can have one or more RPs, and each RP must be configured with a list of multicast groups that it is responsible for.

5. **Shared Tree**

MSDP allows for the creation of shared trees that connect multiple PIM domains. Shared trees are used to forward multicast traffic between PIM domains, and they are built by joining the multicast group at the RP.

Overall, MSDP is an important protocol for enabling multicast traffic to flow between different PIM domains. It provides a way for MSDP Peers to discover active multicast sources in other domains and to forward multicast traffic between domains using shared trees. MSDP helps to reduce unnecessary multicast traffic by allowing for the creation of shared trees and by limiting the scope of multicast traffic to only those PIM domains that have active receivers.

Configuring MSDP

Configuring MSDP involves the following steps:

1. Enable PIM on the routers that will participate in MSDP.
2. Configure the Rendezvous Points (RPs) in each PIM domain. The RP is the root of the shared tree for a particular multicast group.
3. Configure the MSDP peer relationships between MSDP Speakers in different PIM domains. Each MSDP Speaker must be configured with the IP address of its MSDP peers.
4. Configure the MSDP SA filters. SA filters determine which SA messages are forwarded by an MSDP Speaker. You can use SA filters to limit the scope of SA messages and reduce unnecessary multicast traffic.

Here’s an example configuration for MSDP:

```
Router(config)# ip multicast-routing
Router(config)# interface Ethernet0/0
Router(config-if)# ippim sparse-mode
Router(config)# access-list 10 permit 239.1.1.0 0.0.0.255
Router(config)# access-list 10 permit 239.1.2.0 0.0.0.255
Router(config)# ippimrp-address 10.1.1.1 group-list 10
Router(config)# msdp peer 192.168.1.1 connect-source Loopback0
Router(config)# msdp originator-id Loopback0
Router(config)# msdpsa-filter 10 deny 239.1.2.0/24
```

In this configuration, we enable multicast routing on the router and enable PIM sparse-mode on the Ethernet0/0 interface. We then configure an access-list to permit traffic for the multicast groups 239.1.1.0/24 and 239.1.2.0/24.

Next, we configure the RP address for the multicast group 239.1.1.0/24 as 10.1.1.1 and apply the group-list 10 to limit the scope of the RP.

We then configure an MSDP peer relationship with the IP address 192.168.1.1 and specify the source interface as Loopback0. We also configure the MSDP originator ID as Loopback0.

Finally, we configure an SA filter to deny SA messages for the multicast group 239.1.2.0/24. This will prevent SA messages for this group from being forwarded by the MSDP Speaker.

Q18. Explain about MOSPF protocol.

Ans :

Meaning

Multicast Open Shortest Path First (MOSPF) is the extension of the Open Shortest Path First (OSPF) protocol, which is used in unicastrouting.

It also uses the sourcebased tree approach to multicasting. If the internet is running a unicast link-state routing algorithm, the idea can be extended to provide a multicast link-state routing algorithm.

Each router in the internet has a link-state database (LSDB) that can be used to create a shortest-path tree. To extend unicasting to multicasting, each router needs to have another database, as with the case of unicast distance-vector routing, to show which interface has an active member in a particular group.

Now a router goes through the following steps to forward a multicast packet received from source S and to be sent to destination G,

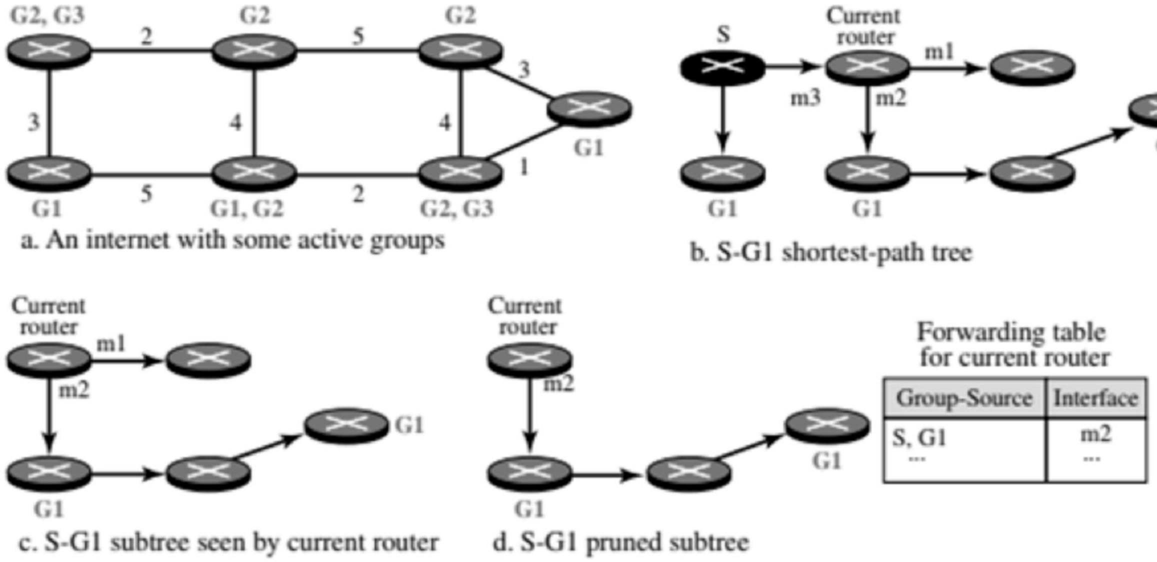
1. The router uses the Dijkstra algorithm to create a shortest-path tree with S (Source) as the root and all destinations in the internet as the leaves. Note that this shortest-path tree is different from the one the router normally uses for unicast forwarding, in which the root of the tree is the router itself. In this case, the root of the tree is the source of the packet defined in the source address of the packet. The router is capable of creating this tree because it has the LSDB, the whole topology of the internet; the Dijkstra algorithm can be used to create a tree with any root, no matter which router is using it. The point we need to remember is that the shortest-path tree created this way depends on the specific source. For each source we need to create a different tree.

2. The router finds itself in the shortest-path tree created in the first step. In other words, the router creates a shortest-path subtree with itself as the root of the subtree.

3. The shortest-path subtree is actually a broadcast subtree with the router as the root and all networks as the leaves. The router now uses a strategy similar to the one we describe in the case of DVMRP to prune the broadcast tree and to change it to a multicast tree. The IGMP protocol is used to find the information at the leaf level. MOSPF has added a new type of link state update packet that floods the membership to all routers. The router can use the information it receives in this way and prune the broadcast tree to make the multicast tree.

4. The router can now forward the received packet out of only those interfaces that correspond to the branches of the multicast tree. We need to make certain that a copy of the multicast packet reaches all networks that have active members of the group and that it does not reach those networks that do not.

   Below figure shows an example of using the steps to change a graph to a multicast tree. For simplicity, we have not shown the network, but we added the groups to each router. The figure shows how a source-based tree is made with the source as the root and changed to a multicast subtree with the root at the current router.



a. An internet with some active groups

b. S-G1 shortest-path tree

c. S-G1 subtree seen by current router

d. S-G1 pruned subtree

Group-Source	Interface
S, G1 ...	m2 ...

Example of tree formation in MOSPF

4.4.6 Spanning Tree Algorithm

Q19. Explain Spanning Tree algorithm working principle.

Ans : **(Imp.)**

Meaning

Spanning Tree Protocol (STP) is a communication protocol operating at data link layer the OSI model to prevent bridge loops and the resulting broadcast storms. It creates a loop " free topology for Ethernet networks.

Working Principle

A bridge loop is created when there are more than one paths between two nodes in a given network. When a message is sent, particularly when a broadcast is done, the bridges repeatedly rebroadcast the same message flooding the network. Since a data link layer frame does not have a time-to-live field in the header, the broadcast frame may loop forever, thus swamping the channels.

Spanning tree protocol creates a spanning tree by disabling all links that form a loop or cycle in the network. This leaves exactly one active path between any two nodes of the network. So when a message is broadcast, there is no way that the same message can be received from an alternate path. The bridges that participate in spanning tree protocol are often called spanning tree bridges.

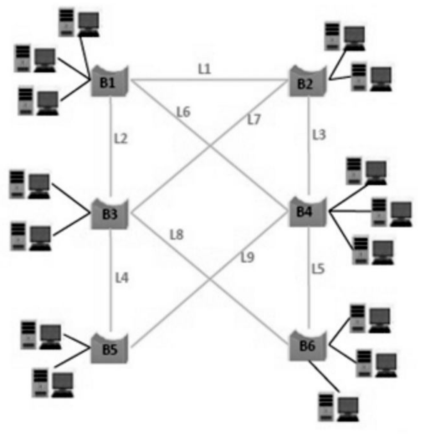
To construct a spanning tree, the bridges broadcast their configuration routes. Then they execute a distributed algorithm for finding out the minimal spanning tree in the network, i.e. the spanning tree with minimal cost. The links not included in this tree are disabled but not removed.

In case a particular active link fails, the algorithm is executed again to find the minimal spanning tree without the failed link. The communication continues through the newly formed spanning tree. When a failed link is restored, the algorithm is re-run including the newly restored link.

Example

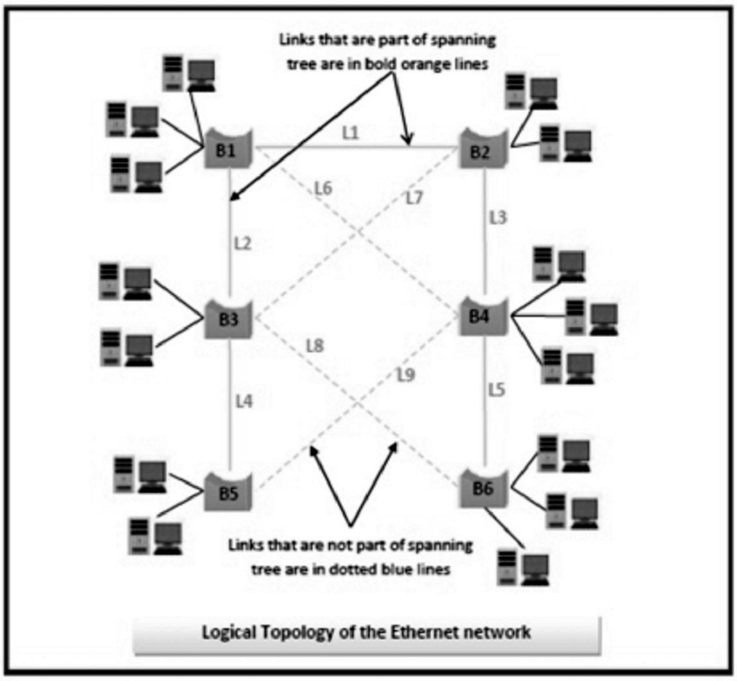
Let us consider a physical topology, as shown in the diagram, for an Ethernet network that comprises of six interconnected bridges. The bridges are named {B1, B2, B3, B4, B5, B6} and several nodes are connected to each bridge. The links between two bridges are named {L1, L2, L3, L4, L5, L6, L7, L8, L9}, where L1 connects B1 and B2, L2 connects B1 and B3 and so on. It is assumed that all links are of uniform costs.

From the diagram we can see that there are multiple paths from a bridge to any other bridge in the network, forming several bridge loops that makes the topology susceptible to broadcast storms.

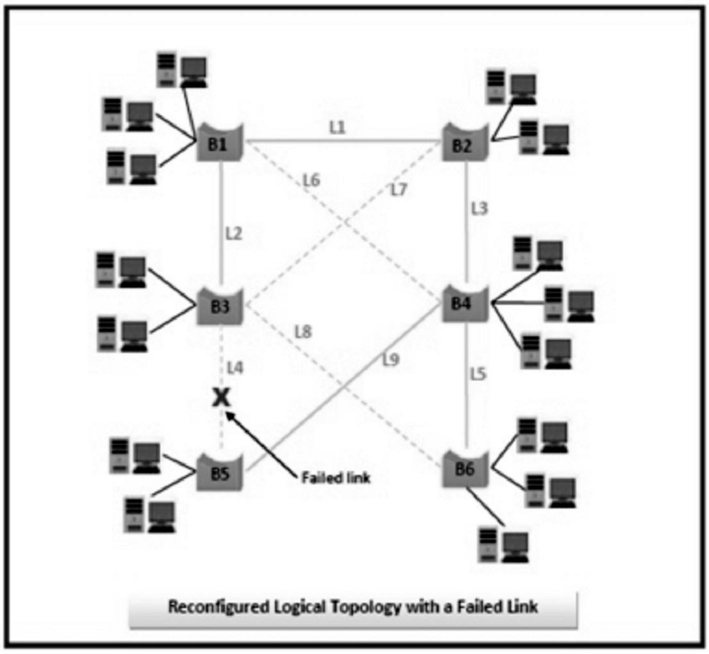


Physical Topology of an Ethernet network

According to spanning tree protocol, links that form a cycle are disabled. Thus, we get a logical topology so that there is exactly one route between any two bridges. One possible logical topology is shown in the following diagram below containing links {L1, L2, L3, L4, L5}-


Links that are part of spanning tree are in bold orange lines
B1
B2
B3
B4
B5
B6
L1
L2
L3
L4
L5
L6
L7
L8
L9
Links that are not part of spanning tree are in dotted blue lines
Logical Topology of the Ethernet network

In the above logical configuration, if a situation arises such that link L4 fails. Then, the spanning tree is reconstituted leaving L4. A possible logical reconfiguration containing links {L1, L2, L3, L5, L9} is as follows -



Short Question & Answers

1. What is congestion control?

Ans :

Meaning

Congestion Control is a type of network layer issue, and it is concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, and there are no lost packets.

Causes

The main cause of congestion is a huge amount of data traffic. But other factors are equally important for making congestion as given below:

1. Sudden arrival of large data (called burst data) from many input lines and trying to access a single output line of a router. In this case, the particular output line is blocked if its bandwidth isn't sufficiently high.
2. Low bandwidth line will produce congestion even if the data rate isn't too high.

2. Principles of **Congestion Control.**

Ans :

1. Monitoring network traffic

Network congestion can occur when there is more traffic on the network than the network can handle. Therefore, it is essential to monitor network traffic continuously to detect congestion before it becomes a problem.

2. Feedback-based mechanisms

Feedback-based mechanisms are used to control the rate of traffic flow and prevent congestion. These mechanisms involve sending feedback messages to the source of the traffic, indicating the current network conditions and the need to reduce the rate of traffic.

3. Resource allocation

Congestion control involves allocating network resources, such as bandwidth and buffer space, effectively. This ensures that each flow of traffic receives a fair share of network resources and prevents any one flow from monopolizing the network.

4. Congestion avoidance

Congestion avoidance techniques are used to prevent congestion from occurring in the first place. These techniques involve detecting and reacting to early signs of congestion, such as packet loss or delay, and reducing the rate of traffic to prevent congestion from occurring.

5. Traffic prioritization

Congestion control involves prioritizing traffic based on its importance and criticality. This ensures that critical traffic, such as voice or video traffic, is given priority over less critical traffic, such as file downloads.

3. What is Routing?

Ans :

Meaning

Routing is the process of directing network traffic from its source to its destination across a network. It is a fundamental concept in computer networking that enables devices on a network to communicate with each other by forwarding packets of data between them. The routing process involves the use of routing protocols and algorithms that determine the optimal path for data to travel from the source to the destination based on various factors, such as network topology, available bandwidth, and network congestion.

Routing can occur at different layers of the networking stack, including the physical layer, data link layer, network layer, and transport layer. At the network layer, routing is typically performed by devices such as routers, which use routing tables and algorithms to determine the best path for data to travel between networks.

4. Write the differences between Inter domain and Intradomain Routing.

Ans :

The following table highlights the major differences between interdomain and intradomain routing protocols.

S.No	Intradomain Routing	Interdomain Routing
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.
3.	Protocols used in intradomain routing are known as Interior-gate way protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.
4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.
5.	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).

5. RIP.

Ans :

RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing tables.

➢ RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.

- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.

6. Disadvantages of RIP.

Ans :

- The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
- It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
- It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
- The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.

7. OSPF protocol.

Ans :

The OSPF stands for Open Shortest Path First. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB.

8. Explain BGP protocol.

Ans :

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

There are many versions of BGP, such as:

- BGP version 1: This version was released in 1989 and is defined in RFC 1105.
- BGP version 2: It was defined in RFC 1163.
- BGP version 3: It was defined in RFC 1267.
- BGP version 4: It is the current version of BGP defined in RFC 1771.

9. Distance Vector Multicast Routing Protocol.

Ans :

The distance vector multicast routing protocol is multicast routing protocol that takes the routing decision based upon the source address of the packet.

- This algorithm constructs the routing tree for a network.
- Whenever a router receives a packet, it forwards it to some of its ports based on the source address of packet.

2. It must prevent the formation of duplicate packets.
3. It must ensure that the path traveled by a packet is the shortest from its source to the router.
4. It should provide dynamic membership.

10. Reverse Path Forwarding.

Ans :

- In this strategy, the router only forwards those packets that have traveled the shortest path from source to destination.
- To achieve this, the router pretends that it has a packet to send to the source from where the packet has arrived.
- In this way, the shortest path to the sender of the packet is computed.
- If the same route is followed by the received packet, it is forwarded to the next router and it is discarded otherwise.
- The reverse path forwarding ensures that the network receives a copy of the packet without formation of loops. A loop occurs when a packet that has left the router may come back again from another interface or the same interface and be forwarded again.

11. Reverse Path Broadcasting.

Ans :

- In order to solve the problem, RPB is used.
- In this method, one parent router is defined for each network.
- The network could accept the multicast packets from this parent router only.
- This router sends packets to those ports for which it is designated as parent.
- Thus, RPB principle' allows a router to broadcast the packet in the network.

This creates duplicate packets on the network and reduces the network efficiency.

12. Multicast Open Shortest Path First.

Ans :

- Multicast open shortest path first is the multicast version of open shortest path first protocol.
- It is an extension of OSPF that uses multicast link state routing method to create source based trees.
- The method used by MOSPF is different from DVMRP.
- The first difference is· that in this method, the tree is least cost tree instead of shortest path tree.
- The second difference is that the tree is not made gradually. It is made immediately it is prepared and ready to use.

13. PIM –DM protocol.

Ans :

PIM-DM (Protocol Independent Multicast - Dense Mode) is a multicast routing protocol that is used to efficiently distribute multicast traffic in a dense network with high bandwidth connectivity. It is a flood-and-prune protocol, which means that multicast traffic is initially flooded to all connected networks and then pruned back based on the network topology and multicast group membership.

In PIM-DM, multicast traffic is forwarded to all directly connected networks until it reaches a network where there are receivers interested in the traffic. Once a receiver is found, the multicast traffic is forwarded only to those networks that have receivers for that multicast group. PIM-DM builds a multicast distribution tree that is rooted at the source and extends to all receivers.

PIM-DM uses a reverse path forwarding (RPF) algorithm to prevent loops and to ensure that multicast traffic is forwarded in the direction of the root of the multicast tree. PIM-DM also uses a prune mechanism to remove branches of the multicast tree where there are no receivers.

Choose the Correct Answers

1. In _______ congestion control, policies are applied to prevent congestion before it happens. [a]

   (a) Open-loop (b) Closed-loop

   (c) Either (a) or (b) (d) Neither (a) nor (b)

2. In _______ we try to avoid traffic congestion. [a]

   (a) Congestion control (b) Quality of service

   (c) Either (a) or (b) (d) Both (a) and (b)

3. Which type of routing protocol is typically used within a single organization or company? [a]

   (a) Intra-domain routing protocol (b) Inter-domain routing protocol

   (c) Both a and b (d) None of the above

4. Among the following which is inter-domain protocol [c]

   (a) RIP (b) OSPF

   (c) BGP (d) All the above

5. Among the following which is multicast routing protocol [d]

   (a) RIP (b) OSPF

   (c) BGP (d) DVMRP

6. Amongth following which protocol uses path-vector routing [c]

   (a) RIP (b) OSPF

   (c) BGP (d) DVMRP

7. Which PIM mode is typically used in networks with a high density of multicast traffic? [a]

   (a) Dense mode (b) Sparse mode

   (c) Source-specific multicast (SSM) mode (d) Any-source multicast (ASM) mode

8. Which PIM mode is typically used in networks with a low density of multicast traffic? [b]

   (a) Dense mode (b) Sparse mode

   (c) Source-specific multicast (SSM) mode (d) Any-source multicast (ASM) mode

9. Which of the following is true about MOSPF routers? [c]

   (a) They are used to discover multicast sources in a single network domain

   (b) They are used to discover multicast sources across multiple network domains

   (c) They are used to establish the best path for multicast traffic to reach its destination

   (d) None of the above

10. What is the purpose of the Root Bridge in Spanning Tree Protocol? [c]

    (a) To serve as the central switch in the network

    (b) To ensure all switches are synchronized

    (c) To determine the shortest path to all switches in the network

    (d) None of the above

Fill in the blanks

1. _______is a technique that regulates the flow of network traffic by smoothing out bursts of traffic and ensuring that traffic flows within defined limits.
2. The packet sent by a node to the source to inform it of congestion is called _______
3. _______ is a technique used to prevent congestion by selectively dropping packets before congestion occurs
4. _______ is the process of directing network traffic from its source to its destination across a network.
5. When several routers are attached in a network, they are known as a _______ link.
6. Full form of MOSPF_______
7. The _______ protocol is a group-shared protocol that uses a core as the root of the tree.
8. _______ protocol for managing multicast traffic across multiple network domains
9. _______ is a communication protocol operating at data link layer the OSI model to prevent bridge loops and the resulting broadcast storms.
10. _______ protocol is used to discover multicast sources across multiple network domains

Answers

1. Traffic shaping
2. Choke
3. Random Early Detection
4. Routing
5. Transient
6. Multicast Open Shortest Path First
7. Core-Based Tree (CBT)
8. PIM
9. Spanning Tree Protocol (STP)
10. MSDP

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.

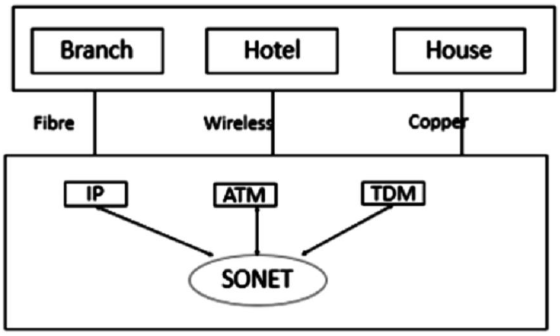
Ans : **(Imp.)**

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

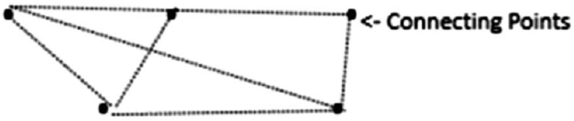
The transport services for the metro are provided by the optical layer. The optical layer has been now giving services for synchronous transmission and performance monitoring.

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.

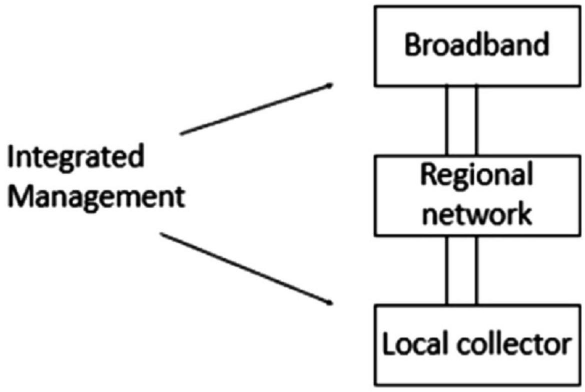
Step 6 :

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 :

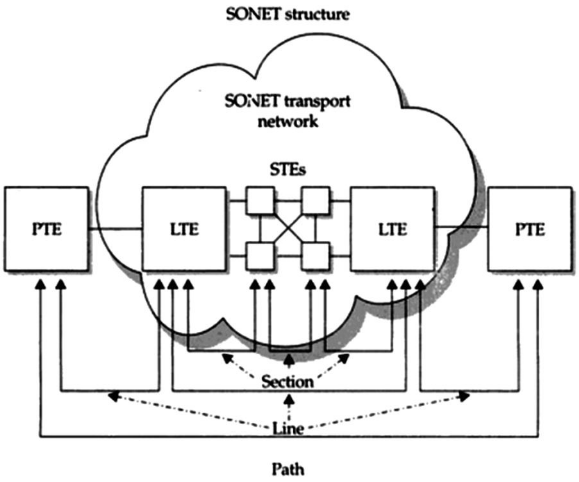
- Increases revenues
- Improved services.
- Reduced operating cost.
- Centralized management.
- Reduced capital investment.

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.

Ans : **(Imp.)**

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.

Ans ; **(Imp.)**

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.

Ans : **(Imp.)**

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.

Ans : **(Imp.)**

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.

Ans : **(Imp.)**

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.

Ans : **(Imp.)**

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.

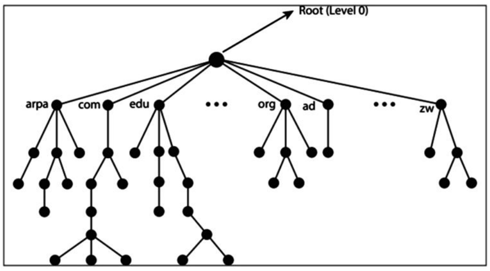


Fig.: Domain Name Space

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.

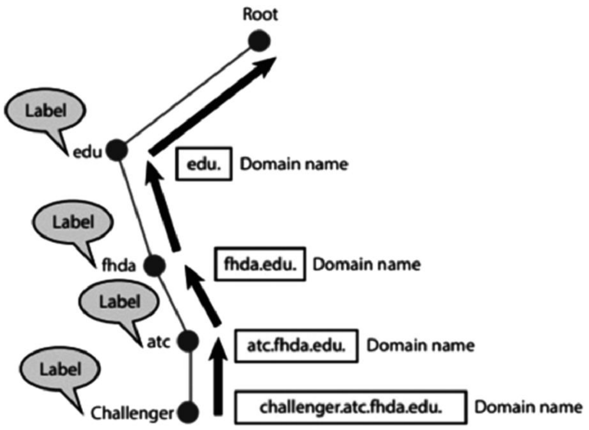


Fig.: Domain Name and Label

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.

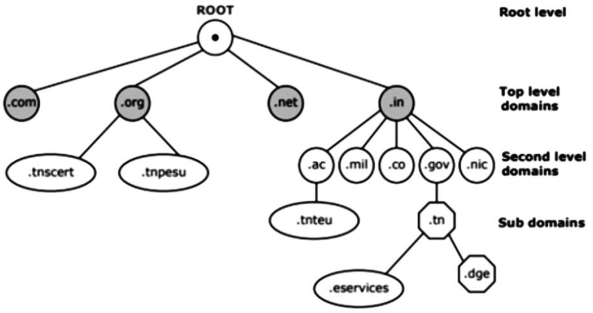


Fig.: Domain representation of www.tnscert.org

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.wikipe dia.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-readable 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.

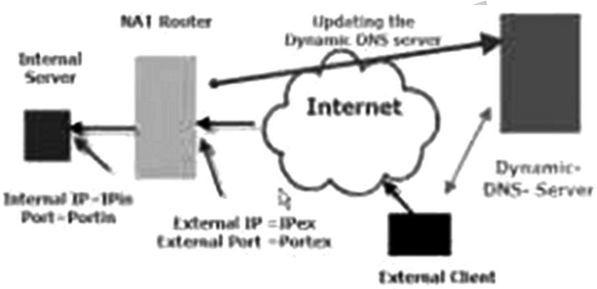
2. **Dynamic DNS service:** The client software communicates with a dynamic DNS service provider, such as DynDNS, No-IP, or DuckDNS, to register a domain name and update the IP address associated with the domain name whenever it changes.

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.


NA1 Router
Updating the Dynamic DNS server
Internal Server
Internet
Dynamic-DNS- Server
Internal IP - IPin Port - Portin
External IP = IPex External Port = Portex
External Client

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.

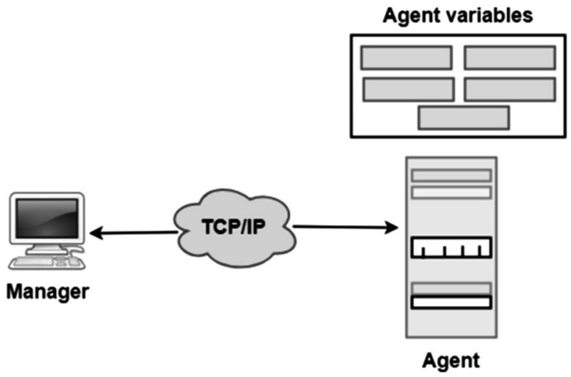
5.3.9 SNMP

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

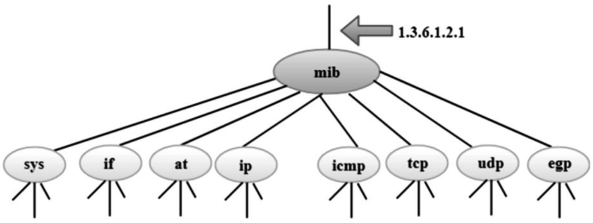
- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is 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.

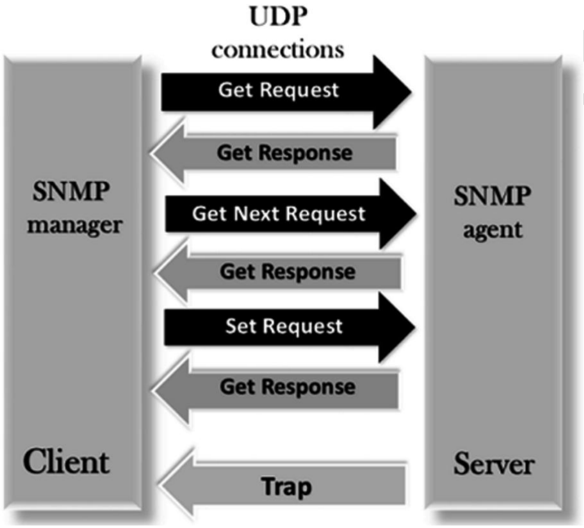
MIB

- 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:

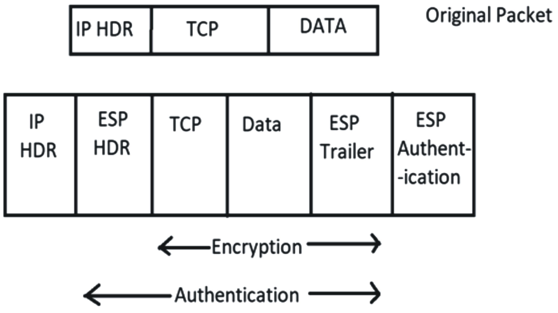
1. **Encapsulating Security Payload (ESP):** It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

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.

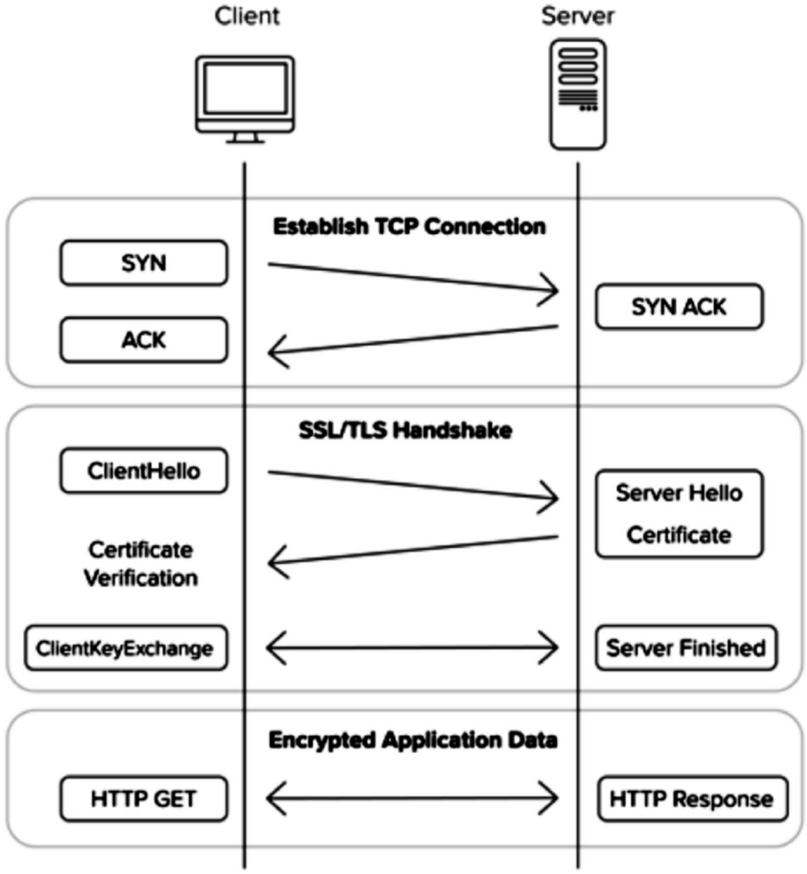
Here are the basic steps involved in an SSL connection:

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

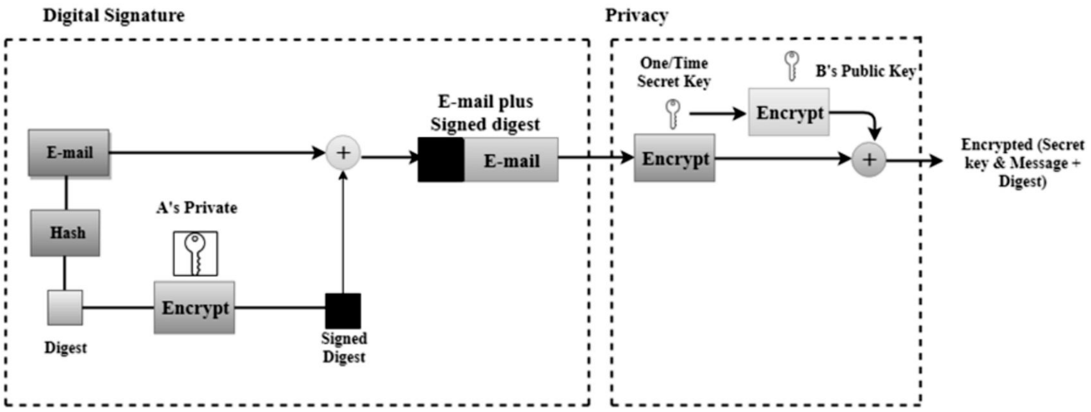
- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) 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.

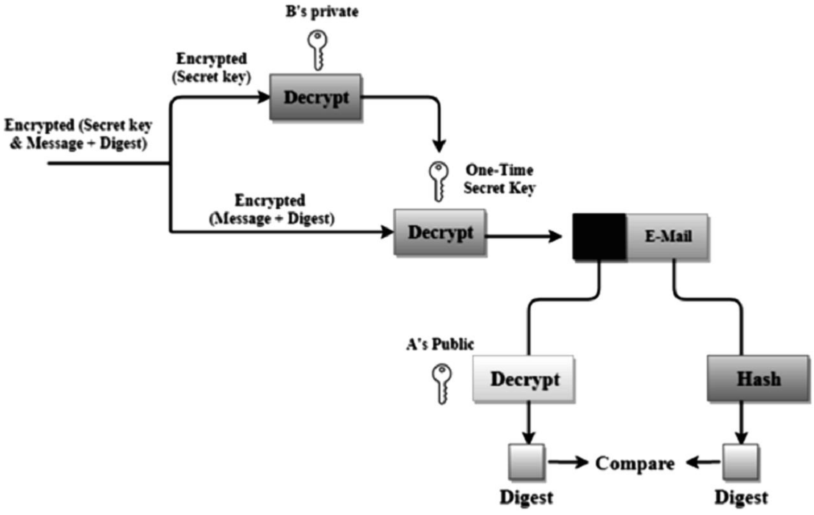
PGP at the Sender site (A)



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.

Ans ; **(Imp.)**

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.

Choose the Correct Answers

1. Among the following which level supports the triple bandwidth. [c]

   (a) OC-1 (b) OC-2

   (c) OC-3 (d) OC-12

2. What is the primary goal of traffic engineering? [b]

   (a) To increase network capacity (b) To reduce network congestion

   (c) To improve network security (d) To improve network reliability

3. Which of the following is a key component of traffic engineering? [b]

   (a) Network topology optimization (b) Quality of Service(QoS) implementation

   (c) Advanced encryption techniques (d) None of the above

4. Which of the following is a characteristic of traffic engineering? [b]

   (a) It is a one-time activity

   (b) It requires continuous monitoring and optimization

   (c) It is not relevant for small-scale networks

   (d) None of the above

5. Among the following which protocol used for streaming multimedia content over the internet [d]

   (a) TCP (b) RTP

   (c) DASH (d) HLS

6. Among the following which method involves saving multimedia content onto a recipient's device for later playback. [b]

   (a) transmission (b) downloading

   (c) uploading (d) attaching

7. What does DNS stand for? [b]

   (a) Domain Name Server (b) Domain Name Service

   (c) Distributed Name Server (d) Distributed Name Service

8. Which of the following is a characteristic of the DNS system? [b]

   (a) It is a centralized system (b) It is a distributed system

   (c) It is a peer-to-peer system (d) None of the above

9. Which of the following is a component of the SNMP system? [d]

   (a) SNMP agent (b) SNMP manager

   (c) Management Information Base (MIB) (d) All of the above

10. What is the primary purpose of SSL/TLS? [a]

    (a) To secure network traffic (b) To optimize network performance

    (c) To manage network devices (d) To encrypt network data

Fill in the Blanks

1. _______ offers cost effective transport both in the access area and core of the network.

2. _______ determining the amount of traffic that will be carried over the network and the capacity that will be required to handle this traffic.

3. _______ is a protocol used to improve the performance and efficiency of network traffic.

4. _______ refers to the time it takes for a data packet to travel from its source to its destination.

5. _______ involves sending multimedia content over the internet in real-time, allowing the recipient to access the content as it is being transmitted.

6. _______ converts analog voice signals into digital data packets, which can be transmitted over the internet using IP networks.

7. Sending multimedia content from a sender's device to a remote server or other recipient's device is called _______.

8. SNMP stands for _______.

9. _______ is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.

10. _______ protocol used to provide secure communication over the internet.

ANSWERS

1. SONET
2. traffic sizing
3. Multiprotocol Label Switching
4. Latency
5. Streaming
6. VOIP
7. uploading
8. Simple Network Management Protocol
9. Internet Key Exchange (IKE)
10. SSL

FACULTY OF INFORMATICS

BCA I-Year, II-Semester (CBCS) Examination

Model Paper - I

ADVANCED COMPUTER NETWORKS

Time : 3 Hours] **[Max. Marks : 70**

Note : Answer all questions from Part - A, & any five questions from Part - B Choosing one questions from each unit.

PART - A (10 × 2 = 20 Marks)

ANSWERS

1. (a) Latency. **(Unit-I, SQA-2)**

(b) FDDI. **(Unit-I, SQA-4)**

(c) Broadband integrated services. **(Unit-II, SQA-9)**

(d) Message Switching. **(Unit-II, SQA-4)**

(e) ICMP Protocol. **(Unit-III, SQA-10)**

(f) IPv4. **(Unit-III, SQA-2)**

(g) What is congestion control? **(Unit-IV, SQA-1)**

(h) Write the differences between Inter domain and Intradomain Routing. **(Unit-IV, SQA-4)**

(i) Reliability. **(Unit-V, SQA-8)**

(j) Characteristics of traffic engineering. **(Unit-V, SQA-4)**

PART - B (5 × 10 = 50 Marks)

UNIT - I

2. Explain about bandwidth and Latency. **(Unit-I, Q.No.2)**

OR

3. Explain Sliding window protocol. **(Unit-I, Q.No.8)**

UNIT - II

4. Explain about circuit switched networks. **(Unit-II, Q.No.1)**

OR

5. Write about broadband integrated services. **(Unit-II, Q.No.10)**

UNIT - III

6. What is class full addressing? Explain. **(Unit-III, Q.No.3)**

OR

7. Why is Fragmentation Needed? **(Unit-III, Q.No.8)**

UNIT - IV

8. Write the differences between Inter domain and Intradomain Routing. **(Unit-IV, Q.No.4)**

OR

9. Explain about OSPF Packets. **(Unit-IV, Q.No.8)**

UNIT - V

10. Explain dynamic domain name system with examples. **(Unit-V, Q.No.17)**

OR

11. What is SONET/SDH? Write SONET/SDH Transmission Standard. **(Unit-V, Q.No.1)**

FACULTY OF INFORMATICS

BCA I-Year, II-Semester (CBCS) Examination

Model Paper - II

ADVANCED COMPUTER NETWORKS

Time : 3 Hours] **[Max. Marks : 70**

Note : Answer all questions from Part - A, & any five questions from Part - B Choosing one questions from each unit.

PART - A (10 × 2 = 20 Marks)

			ANSWERS
1.	(a)	Bandwidth.	**(Unit-I, SQA-1)**
	(b)	Multi access networks.	**(Unit-I, SQA-9)**
	(c)	Asynchronous Transfer Mode.	**(Unit-II, SQA-7)**
	(d)	Explain about circuit switched networks	**(Unit-II, SQA-1)**
	(e)	What is Fragmentation in Networking? Explain.	**(Unit-III, SQA-7)**
	(f)	Address space.	**(Unit-III, SQA-1)**
	(g)	What is Routing?	**(Unit-IV, SQA-3)**
	(h)	Disadvantages of RIP.	**(Unit-IV, SQA-6)**
	(i)	Traffic engineering.	**(Unit-V, SQA-2)**
	(j)	Multiprotocol Label Switching.	**(Unit-V, SQA-6)**

PART - B (5 × 10 = 50 Marks)

UNIT - I

2. Explain about multi access networks. **(Unit-I, Q.No.9)**

OR

3. Write about peer to peer network. **(Unit-I, Q.No.12)**

UNIT - II

4. Explain the benefits and Limitations of Circuit Switching. **(Unit-II, Q.No. 2)**

OR

5. What is Asynchronous Transfer Mode (ATM)? Expalin. **(Unit-II, Q.No. 8)**

UNIT - III

6. What is Network Address Translation? Explain. **(Unit-III, Q.No.5)**

OR

7. Explain the structure of IPV6. **(Unit-III, Q.No.10)**

UNIT - IV

8. What is Routing? Explain Intra- Domain And Inter-domain Routings. **(Unit-IV, Q.No.3)**

OR

9. Explain OSPF protocol. **(Unit-IV, Q.No.7)**

UNIT - V

10. Write about the availability aspect in traffic engineering. **(Unit-V, Q.No.8)**

OR

11. Write about time and delay considerations of traffic egineeering. **(Unit-V, Q.No.6)**

FACULTY OF INFORMATICS

BCA I-Year, II-Semester (CBCS) Examination

Model Paper - III

ADVANCED COMPUTER NETWORKS

Time : 3 Hours] **[Max. Marks : 70**

Note : Answer all questions from Part - A, & any five questions from Part - B Choosing one questions from each unit.

PART - A (10 × 2 = 20 Marks)

ANSWERS

1. (a) ATM. **(Unit-I, SQA-3)**

(b) Frame Relay. **(Unit-I, SQA-5)**

(c) Write Differences between Virtual Circuits & Datagram Networks. **(Unit-II, SQA-3)**

(d) Drawbacks of ATM network. **(Unit-II, SQA-6)**

(e) Advantages of NAT. **(Unit-III, SQA-5)**

(f) What is Checksum? How to apply check-sum for error detection? Explain. **(Unit-III, SQA-8)**

(g) OSPF protocol. **(Unit-IV, SQA-7)**

(h) Distance Vector Multicast Routing Protocol. **(Unit-IV, SQA-9)**

(i) SONET/SDH. **(Unit-V, SQA-1)**

(j) Traffic Sizing. **(Unit-V, SQA-3)**

PART - B (5 × 10 = 50 Marks)

UNIT - I

2. State the applications of P2P Network. **(Unit-I, Q.No.13)**

OR

3. What are different types of errors? Explain error detection techniques. **(Unit-I, Q.No.5)**

UNIT - II

4. Explain briefly about Datagram Networks. **(Unit-II, Q.No. 3)**

OR

5. Write the benefits and Drawbacks of ATM network. **(Unit-II, Q.No. 7)**

UNIT - III

6. Explain about Reverse Address Resolution Protocol. **(Unit-III, Q.No.16)**

OR

7. Explain about IPv6 packet format and extension headers. **(Unit-III, Q.No.12)**

UNIT - IV

8. Explain PIM –DM protocol. **(Unit-IV, Q.No.14)**

OR

9. Explain about Router attributes. **(Unit-IV, Q.No.10)**

UNIT - V

10. How domain names are distributed in DNS ? Explain. **(Unit-V, Q.No.14)**

OR

11. Explain about the protocols used in traffic engieneering. **(Unit-V, Q.No.5)**