DECODE®

A Guide For Engineering Students

COMPUTER NETWORKS AND SECURITY

(For END SEM Exam - 70 Marks)

SUBJECT CODE : 310244

T.E.(Computer Engineering) Semester - V

© Copyright with Technical Publications
All publishing rights (printed and ebook version) reserved with Technical Publications. No part of this book should be reproduced in any form, Electronic, Mechanical, Photocopy or any information storage and retrieval system without prior permission in writing, from Technical Publications, Pune.

Published by :

TECHNICAL PUBLICATIONS®
SINCE 1991
An Up-Thrust for Knowledge

Amit Residency, Office No.1, 412, Shaniwar Peth,
Pune - 411030, M.S. INDIA Ph.: +91-020-24495496/97
Email : info@technicalpublications.in
Website : www.technicalpublications.in

Printer :
Yogiraj Printers & Binders, Sr.No. 10/1A, Ghule Industrial Estate, Nanded Village Road,
Tal. - Haveli, Dist. - Pune - 411041.

ISBN 978-93-5585-206-9

SPPU 19

852069 [1]

SYLLABUS

Computer Networks and Security - (310244)

Credit :	Examination Scheme :
03	End-Sem (TH) : 70 Marks

Unit III Network Layer

Introduction : Functions of Network layer. **Switching Techniques :** Circuit switching, Message Switching, Packet Switching. **IP Protocol :** Classes of IP (Network addressing), IPv4, IPv6, Network Address Translation, Sub-netting, CIDR. **Network layer Protocols :** ARP, RARP, ICMP, IGMP. **Network Routing and Algorithms :** Static Routing, Dynamic Routing, Distance Vector Routing, Link State Routing, Path Vector. **Routing Protocols :** RIP, OSPF, BGP, MPLS. **Routing in MANET :** AODV, DSR, Mobile IP. **(Chapter - 3)**

Unit IV Transport Layer

Process to Process Delivery, Services, Socket Programming. **Elements of Transport Layer Protocols :** Addressing, Connection establishment, Connection release, Flow control and buffering, Multiplexing, Congestion Control. **Transport Layer Protocols :** TCP and UDP, SCTP, RTP, Congestion control and Quality of Service (QoS), Differentiated services, TCP and UDP for Wireless networks. **(Chapter - 4)**

Unit V Application Layer

Introduction, Web and HTTP, Web Caching, DNS, Email : SMTP, MIME, POP3, Webmail, FTP, TELNET, DHCP, SNMP. **(Chapter - 5)**

Unit VI Security

Introduction, Security services, Need of Security, Key Principles of Security, Threats and Vulnerabilities, Types of Attacks, ITU-T X.800 Security Architecture for OSI, Security Policy and mechanisms, Operational Model of Network Security, Symmetric and Asymmetric Key Cryptography. Security in Network, Transport and Application : Introduction of IPSec, SSL, HTTPS, S/MIME, Overview of IDS and Firewalls. **(Chapter - 6)**

TABLE OF CONTENTS

Unit III

Chapter - 3 Network Layer (3 - 1) to (3 - 54)

3.1 Functions of Network Layer ..... 3 - 1
3.2 Switching Techniques ..... 3 - 4
3.3 IP Protocol ..... 3 - 7
3.4 IPv6 ..... 3 - 16
3.5 Network Layer Protocols : ARP, RARP, ICMP, IGMP ..... 3 - 22
3.6 Network Routing and Algorithms ..... 3 - 33
3.7 Distance Vector Routing ..... 3 - 35
3.8 Link State Routing ..... 3 - 40
3.9 Routing Protocols : RIP, OSPF, BGP ..... 3 - 42
3.10 Routing in MANET ..... 3 - 48
3.11 Mobile IP ..... 3 - 53

Unit IV

Chapter - 4 Transport Layer (4 - 1) to (4 - 41)

4.1 Process to Process Delivery ..... 4 - 1
4.2 Transport Service ..... 4 - 3
4.3 Socket Programming ..... 4 - 6
4.4 Elements of Transport Layer Protocols ..... 4 - 8
4.5 Congestion Control ..... 4 - 13
4.6 Transport Layer Protocols : TCP ..... 4 - 15
4.7 Transport Layer Protocols : UDP, SCTP, RTP ..... 4 - 25
4.8 Congestion Control and Quality of Service (QoS), Differentiated Services ..... 4 - 30
4.9 TCP and UDP for Wireless Networks ..... 4 - 40

Unit V

Chapter - 5 Application Layer (5 - 1) to (5 - 41)

5.1 Web ..... 5 - 1
5.2 HTTP ..... 5 - 5
5.3 Web Caching ..... 5 - 12
5.4 DNS ..... 5 - 13
5.5 Email : SMTP, MIME, POP3 ..... 5 - 19
5.5 FTP ..... 5 - 27
5.7 TELNET ..... 5 - 32
5.8 DHCP ..... 5 - 35
5.9 SNMP ..... 5 - 37

Unit VI

Chapter - 6 Security (6 - 1) to (6 - 39)

6.1 Introduction ..... 6 - 1
6.2 Security Services ..... 6 - 4
6.3 Types of Attacks ..... 6 - 5
6.4 X.800 Security ..... 6 - 10
6.5 Security Policy and Mechanism ..... 6 - 11
6.6 Operational Model of Network Security ..... 6 - 12
6.7 Symmetric Key Cryptography ..... 6 - 13
6.8 Asymmetric Key Cryptography ..... 6 - 22
6.9 Security in Network, Transport and Application ..... 6 - 29
6.10 SSL ..... 6 - 31
6.11 HTTPS and S/MIME ..... 6 - 32
6.12 Overview of IDS and Firewalls ..... 6 - 36

Solved Model Question Papers (M - 1) to (M - 4)

Unit III

3 Network Layer

3.1 : Functions of Network Layer

Q.1 Explain network layer services.

Ans. : • Main Task of the network layer is to move packets from the source host to the destination host. It transport packet from sending to receiving hosts via internet.

- Network layer protocols exist in every host and route. In order to provide this service, the transport layer relies on the services of the network layer, which provides a communication service between hosts.
- In particular, the network layer moves transport-layer segments from one host to another.
- At the sending host, the transport-layer segment is passed to the network layer. It is then the job of the network layer to get the segment to the destination host and pass the segment up the protocol stack to the transport layer.
- Network layer services are packetizing, routing & forwarding and other services.

1. Packetizing

- Encapsulating the payload in a network layer packet at the source and de-capsulating the payload from the network layer packet at the destination called **packetizing**.
- Source host receives the payload from the upper layer protocol, adds a header that contains the source and destination address and some other information that is required by the network layer protocol and delivers the packet to the data link layer.

- The destination host receives the network layer packet from its data link layer, decapsulates the packet and delivers the payload to the corresponding upper layer protocol.

2. Forwarding

- When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.
- Forwarding refers to the way a packet is delivered to the next node. It requires a host or router to have a routing table.
- Forwarding refers to the router local action of transferring a datagram from an input link interface to the appropriate output link interface.
- When host has a packet to send, it looks at routing table to find the route to the final destination.

3. Routing

- Combination of LANs, WANs and routers with interconnected forms physical network. Therefore, there is more than one route from the source to the destination.
- Network layer is responsible for finding the best one among these possible routes that called **routing**.
- The selection of route is generally based on some performance criteria. The simplest criteria is to choose shortest root through the network.

4. Other services

- Network layer provide limited error control but no flow control.
- Congestion may occur it the number of datagrams sent by source computers is beyond the capacity of the network or routers.
- Some congestion control methods are used to solve congestion problem.
- Three important functions of network layer :
  1. Path determination : Route taken by packets from source to destination. Routing algorithms is used for this.
  2. Switching : Move packets from router's input to appropriate router output.

3. Call setup : Some network architectures require router call setup along path before data flows.

Q.2 Describe briefly network layer functions.

Ans. : • The network layer is the lowest one in the OSI model that is concerned with actually getting data from one computer to another even if it is on a remote network; in contrast, the data link layer only deals with devices that are local to each other.

• **Network layer functions :**

1. **Logical addressing :** Every device that communicates over a network has associated with it a logical address, sometimes called a *layer three* address. For example : Internet Protocol (IP) is the network layer protocol and every machine has an IP address.
2. **Routing :** Moving data across a series of interconnected networks is probably the defining function of the network layer.
3. **Datagram encapsulation :** The network layer normally encapsulates messages received from higher layers by placing them into *datagram* with a network layer header.
4. **Fragmentation and reassembly :** The network layer must send messages down to the data link layer for transmission. Some data link layer technologies have limits on the length of any message that can be sent.
5. **Error handling and diagnostics :** Special protocols are used at the network layer to allow devices that are logically connected, or that are trying to route traffic, to exchange information about the status of hosts on the network or the devices themselves.

Q.3 Which types of services provided by network layer to transport layer ?

Ans. : • Network layer provides the services to the transport layer at the network layer/transport layer interface.

• The network layer must fulfill following requirements.

1. The service should be independent of network topology.
2. The network addresses should be made available to the transport with a uniform numbering plan.

3. The transport layer should be shielded from the number, type and topology of the routers present.

3.2 : Switching Techniques

Q.4 State with reasons if circuit switching is better suited for real time traffic.

Ans. : • In circuit switching the channel bandwidth is reserved for an information flow. To ensure timely delivery of the data, the capacity of the circuit has to be at least equal to the peak transmission rate of the flow.

- The circuit is said to be peak allocated, and then the network offers a connection-oriented service with a perfect Quality of Service (QoS) in terms of delay jitter and bandwidth guarantees.
- Contention only occurs when allocating channels to circuits during circuit/call establishment. If there are not enough channels for the request, the call establishment may be delayed, blocked or even dropped. In contrast, once the call is accepted, resources are not shared with other flows, eliminating any uncertainty and, thus, removing the need for buffering, processing or scheduling in the data path.
- When circuits are peak allocated, the only measure of Quality of Service (QoS) in circuit switching is the blocking probability of a call.
- Following are some of reasons :

  1. Higher efficiency 2. Fixed BW 3. Dynamic routing

Q.5 Explain the various types of switching methods with suitable examples.

Ans. : • A switched network is made up of a series of interconnected nodes called switches. Switches divide a network into several isolated channels. Packets sending from 1 channel will not go to another if not specify. Each channel has its own capacity and need not be shared with other channels.

- Three conventional switching methods are packet, circuit and message switching.

1. Packet switching : • Packet switching is often used in computer networks where individual users have need of the channel intermittently. While using the channel the application requires high bandwidth, but most of the time, each user does not require that channel at all.

- Such applications, characterized by a high peak to average requirement for capacity, are called bursty and are ideal for packet switching.
- In packet switching, messages are broken into short blocks and interleaved with other messages. Thus, users queue for the channel and share it with one another efficiently.
- Data is sent in individual packets. Each packet is forwarded from switch to switch, eventually reaching its destination. Each switching node has a small amount of buffer space to temporarily hold packets.
- If the outgoing line is busy, the packet stay in queue until the line becomes available.
- Packet switching handles bursty traffic well.

2. Circuit switching : • Circuit switching is most preferred in telephone networks. Telephone networks are connection before the actual transfer of information can take place.

- An end-to-end path setup beginning of a session, dedicated to the application, and then released at the end of session. This is called circuit switching.
- Circuit switching is effective for application switching is effective for application which make comparatively steady use of channel.

3. Message switching : • Message switching is used to describe the telegraph network. When this form of switching is used, no physical copper path is established in advance between sender and receiver.

- When the sender has a block of data to be sent, it is stored in the first switching office i.e. router and then forwarded later, one hope at a time.
- Each block is received in its entirely, inspected for errors, and then transmitted. A network using this technique is called a store and forward network.

- The message was punched on paper tape off line at the sending office and then read in and transmitted over a communication line to the next office along the way, where it was punched out on paper tape.
- An operator tore the tape off and read it in on one of the many tape readers, one per outgoing trunk. Such a switching office was called a torn tape office.
- With message switching, there is no limit on block size, which means that routers must have disks to buffer long blocks. It also means that a single block may tie up a router, router line for minutes, rendering message switching uses for interactive traffic.
- Message switching does not involve a call setup. It can achieve a high utilization of the transmission line. Message switching is not suitable for interactive applications.

Q.6 Compare circuit switching with packet switching.

Ans. :

Sr. No.	Circuit switching	Packet switching
1.	There is physical connection between transmitter and receiver.	No physical path is established between transmitter and receiver.
2.	All the packet uses same path.	Packet travels independently.
3.	Needs an end to end path before the data transmission.	No needs of end to end path before data transmission.
4.	Reverses the entire bandwidth in advance.	Does not reserve the bandwidth in advance.
5.	Waste of bandwidth is possible.	No waste of bandwidth.
6.	Recording of packet can never happen with circuit switching.	Recording of packet is possible.
7.	Not suitable for handling interactive traffic.	Suitable for handling interactive traffic.
8.	It cannot support store and forward transmission.	It support store and forward transmission.

Q.7 What are the differences between virtual circuit and datagrams ? Why packet switching is preferred in data networks ?

Ans. : Comparison between Virtual Circuit and Datagram

Sr. No.	Virtual circuit	Datagram
1	Circuit setup is required.	Circuit setup is not required.
2	Each packet contains a short VC number as address.	Each packet contains the full source and destination address.
3	Route chosen when VC is setup and all packets follow this route.	Each packet is routed independently.
4	In case of router failure all VC that passed through the router are terminated.	Only crashed packets lost.
5	Congestion control is easy using buffers.	Difficult congestion control.

Packet switching is preferred in data network because :

1. More efficient use of overall network bandwidth due to flexibility in routing the smaller packets over shared links.
2. Packet switching networks are often cheaper to build as less equipment is needed.
3. In packet switching, the transmission bandwidth is dynamically allocated, permitting many users to share the same transmission line previously required for one user.

3.3 : IP Protocol

Q.8 Draw and explain IPV4 header.

☞ **[SPPU : Dec.-19, May-18, End Sem, Marks 8]**

Ans. : • An Internet Protocol (IP) address has a fixed length of 32 bits.

• IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.

- The address structure was originally defined to have a two level hierarchy : network ID and host ID.
- The **network ID** identifies the network the host is connected to. The **host ID** identifies the network connection to the host rather than the actual host.

Header Format

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.
- Fig. Q.8.1 shows IPv4 header format

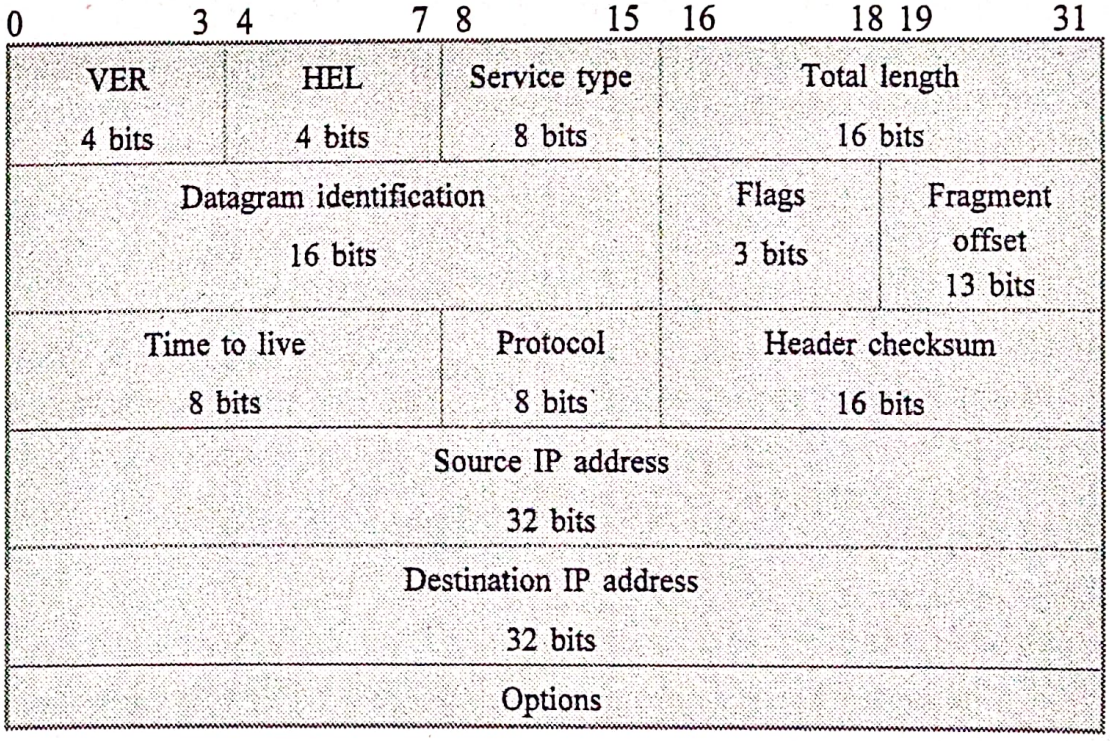


Fig. Q.8.1 IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field. The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).
3. **Service type** : The service type is an indication of the quality of service requested for this IP datagram.
4. **Total length** specifies the total length of the datagram, header and data, in octets.

5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram.
   E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.
11. **Source / Destination IP addresses** are the 32-bit source / destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provides a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tells the routers along the route to put timestamps in the option data.
13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

Q.9 What is IP ? Discuss the different classes of IP addressing ? Explain classfull address.

Ans. : **IP :** IP corresponds to the network layer in the OSI model and provides connectionless best effort delivery services to the transport layer.

Classful addressing : The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

- Fig. Q.9.1 shows the five classes of IP addresses.

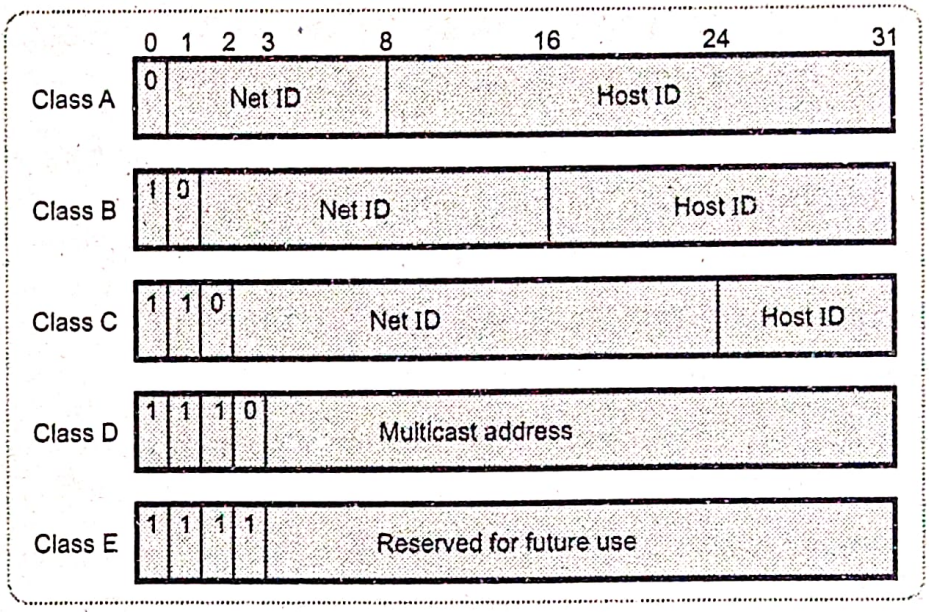


Fig. Q.9.1 Five classes of IP addresses

- Class D addresses are used for multicast services that allow a host to send information to a group of hosts simultaneously. Class E addresses are reserved for future use.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.
- In a class A network, the first byte is assigned to the network address, and the remaining three bytes used for the node addresses. The class A format is

  Network.Node.Node.Node

  For example : 14.28.101.120 in this IP address 14 is the network address and 28.101.120 is the node address.

- In class B network, the first two bytes are assigned to the network address and the remaining two bytes are used for node addresses. The format is

  Network.Network.Node.Node

  For example : 150.51.30.40 in this IP address network address is 150.51 and node address is 30.40.

- In class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is

  Network.Network.Network.Node

- **For example :** 200.20.42.120 in this example 200.20.42 is the network address and 120 is the node address.

Q.10 What do you mean classless addressing ? Explain restriction on classless addressing.

Ans. : • In classless addressing variable length blocks are assigned that belong to no class. In this, the entire address space is divided into blocks of different sizes. An organization is granted a block suitable for its purposes.

- Fig. Q.10.1 shows the architecture of classless addressing.

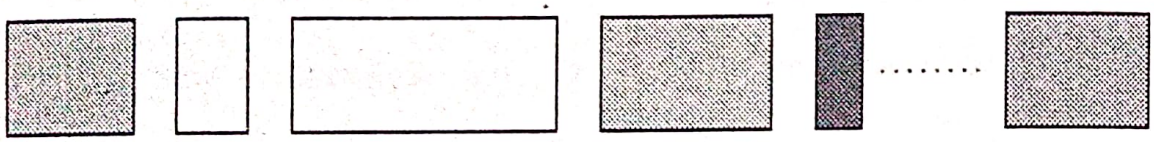


Fig. Q.10.1 Architecture of classless addressing

- In classless addressing, when an entity, small or large, needs to be connected to the internet it is granted a block of addresses. The size of the block varies based on the nature and size of the entity.

Restriction

- To simplify the handling of addresses, the internet authorities impose three restrictions on classless address blocks.
  1. The addresses in a block must be contiguous, one after another.
  2. The number of addresses in a block must be a power of 2.

3. The first address must be evenly divisible by the number of addresses.

- In IPv4 addressing, a block of addresses can be defined as x.y.z.t/n in which x.y.z.t defines one of the addresses and the /n define the mask. The address and the /n notation completely define the whole block.
- IPv4 is the delivery mechanism used by the TCP/IP protocols. IPv4 is an unreliable and connectionless datagram protocol.
- IPv4 is also a connectionless protocol for a packet switching network that uses the datagram approach.

Q.11 Find the sub-network address for the following.

Sr. No.	*IP address*	*Mask*
a)	*141.181.14.16*	*255.255.224.0*
b)	*200.34.22.156*	*255.255.255.240*
c)	*125.35.12.57*	*255.255.0.0*

Ans. :

a)

141.181.14.16	IP address
255.255.224.0	Mask
141.181.0.0	Sub-network address

b)

200.34.22.156	IP address
255.255.255.240	Mask
200.34.22.144	Sub-network address

c)

125.35.12.57	IP address
255.255.0.0	Mask
125.35.0.0	Sub-network address

(i.e. 128) So for byte-3 value use bit-wise AND operator. It is shown below.

120.14.22.16	IP address
255.255.128.0	Mask
120.14.0.0	Sub-network address

In the above example, the bit wise ANDing is done in between 22 and 128. it is as follows

22	Binary representation	0 0 0 1 0 1 1 0
128	Binary representation	1 0 0 0 0 0 0 0
0		0 0 0 0 0 0 0 0

Thus the sub-network address for this is 120.14.0.0.

Q.12 A small organization is given a block with the beginning address and the prefix length 205.16.37.24/29 (in slash notation). What is the range of the block. ? ☞ [SPPU : May-18, End Sem, Marks 4]

Ans. : The binary representation of the given address is

11001101 00010000 00100101 00100110.

1. **First address :** If we set 32 - 28 rightmost bits to 0, we get
   11001101 00010000 00100101 00100000 or 205.16.37.32.
   Hence, the first address in the block is 205.16.37.32.
2. **Last address :** If we set 32 - 28 rightmost bits to 1, we get
   11001101 00010000 00100101 100101111 or 205.16.37.47
   Hence, the last address in the block is 205.16.37.47.
3. **Number of addresses :** The value of n is 28, which means that number of addresses is 2^{32-28} or 16.

Alternate way to find the first address, the last address and the number of addresses are as follows :

1. The first address can be found by ANDing the given addresses with the mask. The result of ANDing 2 bits is 1 if both bits are 1s; the result is 0 otherwise.

Address :	11001101 00010000 00100101 00100110
Mask :	11111111 11111111 11111111 11110000
First address :	11001101 00010000 00100101 00100000

2. The last address can be found by ORing the given addresses with the complement of the mask. The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise.

Address :	11001101 00010000 00100101 00100110
Mask complement :	00000000 00000000 00000000 00001111
Last address :	11001101 00010000 00100101 00101111

3. The number of addresses can be found by complementing the mask and adding 1 to it.

Mask complement :	000000000 00000000 00000000 00001111
Number of addresses :	15 + 1 = 16

Q.13 A host was given the 192.168.2.64 /27 IP address, indicate :
i) Netmask of the network.
ii) The network broadcast address to which th host belongs.
iii) The total number of hosts available in the network.

☞ [SPPU : Dec.-18, 19, End Sem, Marks 8]

Ans. : Netmask of the network = 255.255.255.224

Network Address : 192.168.2.64/27

Broadcast Address : 192.168.2.95

First Host : 192.168.2.65

Last Host : 192.168.2.94

Hosts per Net : 30

Q.14 What is meant by fragmentation ? Is fragmentation needed in concentrated virtual circuit internets or in any datagram system.

Ans. : • Fragmentation means the division of a packet into smaller units to accommodate a protocols MTU. Each network imposes some maximum size on its packet. These limit have various causes, among them. Hardware, US, protocol etc. Fig. Q.14.1 shows the fragmentation.

- Maximum packet size may vary from one network to another. Either the fragmentation and reassembly function can be performed on a per network basis.
- Fragmentation is need in concatenated virtual circuit and datagram systems. Even in concatenated virtual circuit network, some network

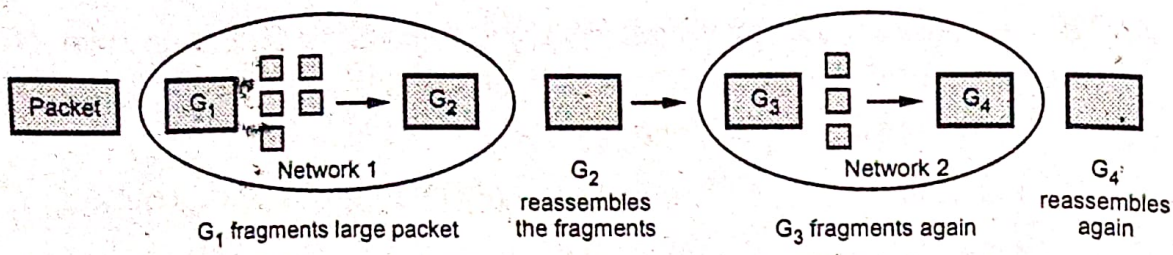


Fig. Q.14.1 Fragmentation

along the path might accept 1024 byte packets and others might only accept 48 byte packets. Fragmentation still needed.

- The Internet is a datagram network. This means that the network layer only provides a datagram service, in the case of the internet, best-effort.
- The network layer doesn't provide reliability or connection services to the transport layer.
- When an IP datagram travels from one host to another, it may pass through different physical networks. Each physical network has a maximum frame size, called Maximum Transmission Unit (MTU), which limits the datagram length.
- A fragment is treated as a normal IP datagram while being transported to their destination. Thus, fragments of a datagram each have a header. If one of the fragments gets lost, the complete datagram is considered lost.
- It is possible that fragments of the same IP datagram reach the destination host via multiple routes. Finally, since they may pass through networks with a smaller MTU than the sender's one, they are subject to further fragmentation.

Q.15 A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets (subnet masks for each subnet, starting address and ending address of each subnet).

☞ [SPPU : April-16, Marks 5]

Ans. : • Site address = 201.70.64.0

- Given IP address is class C address. Default subnet mask for class C is 255.255.255.0
- The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3). We need 3 more 1s in

the subnet mask. The total number of 1s in the subnet mask is 27 (24 + 3).

- The total number of 0s is 5 (32 – 27).
- The mask is 11111111 11111111 11111111 11100000 => 255.255.255.224
- The number of subnets is 8.

  Subnet Mask : 255.255.255.224

- The number of addresses in each subnet is 2^5 = 32.

Subnet Number	Staring Address	Ending Address
Subnet 1	207.70.64.0	207.70.64.31
Subnet 2	207.70.64.32	207.70.64.63
Subnet 3	207.70.64.64	207.70.64.95
Subnet 4	207.70.64.96	207.70.64.127
Subnet 5	207.70.64.128	207.70.64.159
Subnet 6	207.70.64.160	207.70.64.191
Subnet 7	207.70.64.192	207.70.64.223
Subnet 8	207.70.64.224	207.70.64.255

3.4 : IPv6

Q.16 Explain types of address used in IPv6.

Ans. : • IPv6 allows three types of addresses.

1. Unicast 2. Anycast 3. Multicast

1. Unicast : An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2. Anycast : An identifier for a set of interfaces. A packet sent to an anycast address is delivered to one of the interfaces identified by the address.

3. Multicast : An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

- The first field of any IPv6 address is the variable-length format prefix, which identifies various categories of address

Q.17 Draw and explain IPv6 header. Explain the significance of extension header. ☞ [SPPU : Dec.-17, End Sem, Marks 6]

Ans. : • Fig. Q.17.1 shows the IPv6 datagram header format.

| 4 bits | 4 bits | 8 bits | 8 bits | 8 bits |

<table>
<tr><td>VER</td><td>PRI</td><td colspan="3">Flow label</td></tr>
<tr><td colspan="3">Payload length</td><td>Next header</td><td>Hop limit</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td>Next header</td><td colspan="4">Header length</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>Next header</td><td colspan="4">Header length</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>Next header</td><td colspan="4">Header length</td></tr>
<tr><td colspan="5"></td></tr>
</table>

Fig. Q.17.1 IPv6 header

1. **Versions :** This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority :** The 4 bits priority field defines the priority of the packet with respect to traffic congestion.

3. **Flow label :** It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length :** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header :** It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit :** This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address :** The source address field is a 128 bits internet address that identifies the original.
8. **Destination address :** It is 128 bits Internet address that usually identifies the final destination of the datagram.

Extension Headers

- The length of the base header is fixed at 40 bytes. Types of extension headers are

1. Hop by hop option	2. Source routing
3. Fragmentation	4. Authentication
5. Encrypted security payload	6. Destination option

- **Hop by hop option** is used when the source needs to pass information to all routers visited by the datagram.
- **Source routing** extension header combines the concepts of the strict source route and the loose source route options of IPv4.
- The concept of **fragmentation** is the same as that in IPv4. In IPv6, only the original source can fragment.
- The **authentication** header has a dual purpose : It validates the message sender and ensures the integrity of data.
- The **encrypted security payload** is an extension that provides confidentiality and guards against eavesdropping.
- The **destination option** is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

Q.18 Differentiate between IPv4 and IPv6.

☞ [SPPU : May-17, End Sem, Marks 4]

Ans. :

Sr. No.	IPv4	IPv6
1.	Header size is 32 bits.	Header size is 128 bits.
2.	It cannot support autoconfiguration.	Supports autoconfiguration
3.	Cannot support real time application.	Supports real time application.
4.	No security at network layer.	Provides security at network layer.
5.	Throughput and delay is more.	Throughput and delay is less.

Q.19 What is significance of priority and flow label fields in IPv6.

☞ [SPPU : May-15 (End Sem.), Marks 5]

Ans. : Fig. Q.17.1 shows the IPv6 datagram header format. (Refer Q.17)

Significance of Priority Field

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories

1. Congestion controlled
2. Non-congestion controlled

- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. Congestion controlled data are assigned priorities from 0 to 7.

Significance of Flow Label Field

Flow label field is a 24 bits field that is designed to provide special handling for a particular flow of data.

Q.20 Explain transition from IPv4 to IPv6 using tunneling.

☞ [SPPU : Dec.-16 (End Sem), Marks 8]

Ans. : • Three strategies have been devised by the IETF to help the transition.

1. Dual stack 2. Tunneling 3. Header translation

1. Dual stack

- All the host must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.
- Fig. Q.20.1 shows the dual stack.
- To determine which version to use when sending a packet to destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

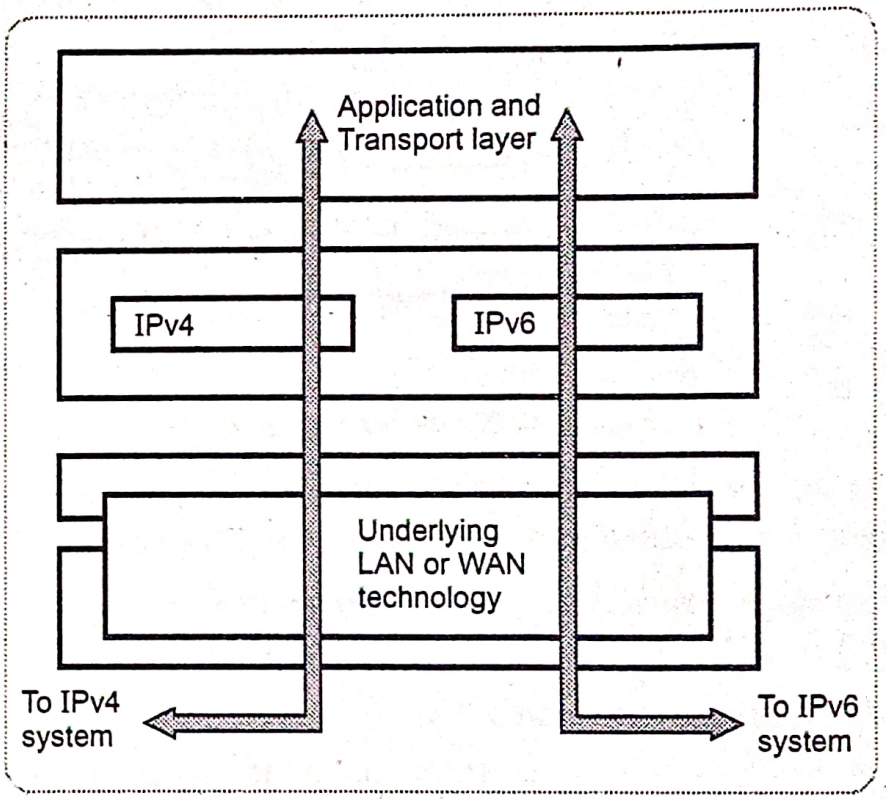


Fig. Q.20.1 Dual stack

2. Tunneling

- When two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. The IPv6

packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.

- Fig. Q.20.2 shows the tunneling.

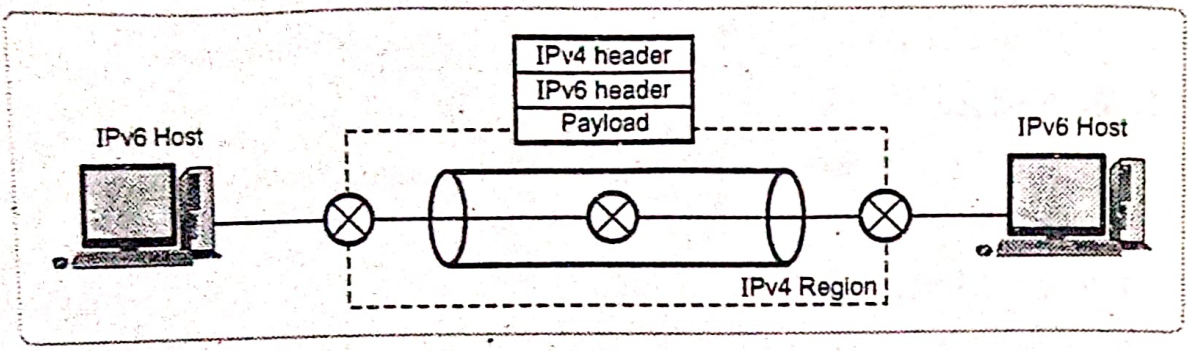


Fig. Q.20.2 Tunneling

3. Header translation

- Header translation is used when some of the system uses IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6.
- Fig. Q.20.3 shows the header translation.

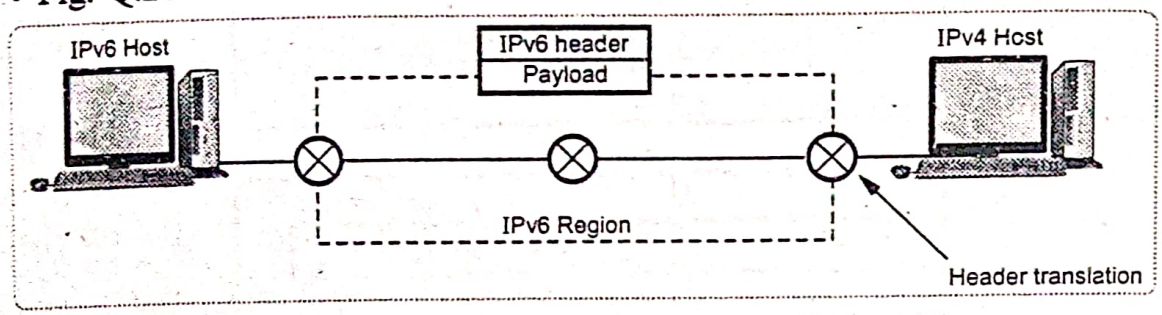


Fig. Q.20.3 Header translation

- The header format must be totally changed through header translation. The header of the IPv6 parket is converted to IPv4 header.

Q.21 Explain Network Address Translation (NAT).

☞ [SPPU : May-18, Dec.-19, End Sem, Marks 4]

OR Write short note on NAT.

☞ [SPPU : Dec.-17,18, May-19, End Sem, Marks6]

Ans. : • Within the company, every machine has a unique address of the form 10 X.Y.Z. when a packet leaves the company premises, it passes through the NAT box that convert the internal IP source address 10.0.0.1. NAT box is often combined in a single device with a firewall. It is also possible to integrate the NAT box into the company router.

- Fig. Q.21.1 shows placement of NAT box.

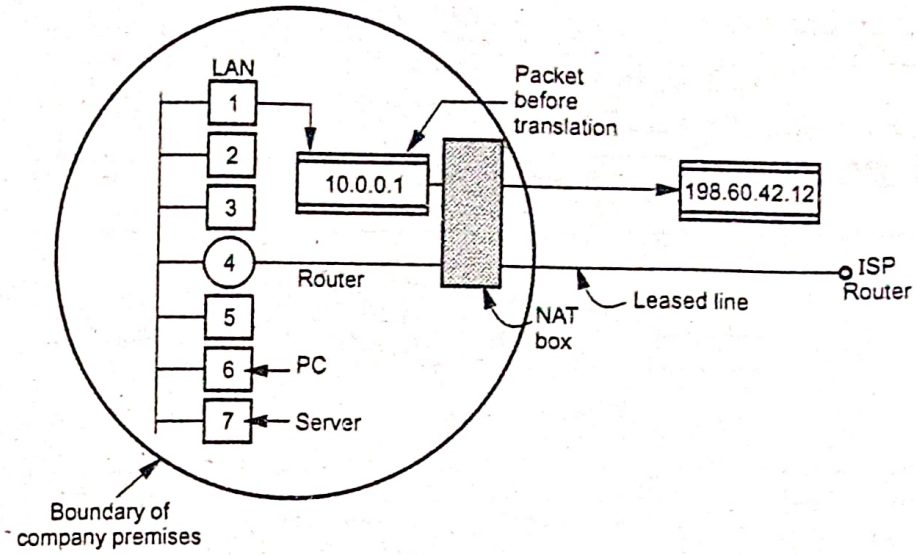


Fig. Q.21.1 NAT

- Whenever an outgoing packet enters the NAT box, the 10.X.Y.Z. SA is replaced by the company true IP address. In, addition, TCP source port field is replaced by an index into the NAT box 65536 entry translation table. This table entry contains the original IP address and original source port. Finally both the IP and TCP header checksums are recomputed and inserted into the packet.
- When process want to establish a TCP connection with a remote process, it attached itself to an unused TCP port on its own machine. This is called a source port and tells the TCP code where to send incoming packets belonging to this connection. The process also supplies a destination port to tell who to give the packet to on the remote side.

3.5 : Network Layer Protocols : ARP, RARP, ICMP, IGMP

Q.22 Explain : Address Resolution Protocol (ARP).

☞ **[SPPU : May-18, Dec.-19, End Sem, Marks 4]**

Ans. : • ARP associates an IP address with its physical address. Anytime a host, or a router needs to find the physical address of another host or router on its network, it sends an ARP query packet. The packet includes the physical address and IP address of the sender and the IP address of the receiver.

- Fig. Q.22.1 shows the operpation of ARP.

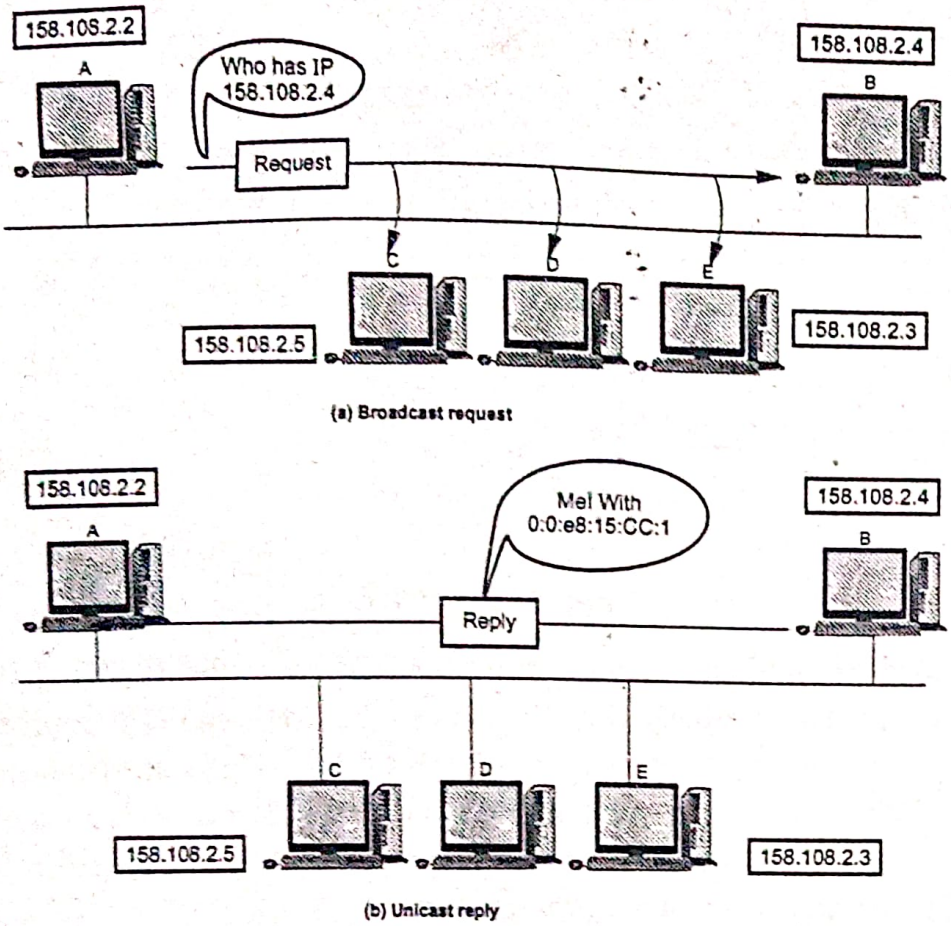


Fig. Q.22.1 ARP operation

- Consider the following example, computer A and computer B share a physical network. Each computer has an assigned IP address I_A and I_B **Physical addresses** P_A and P_B. The goal is to device low-level software that hides physical addresses and allows higher-level programs to work only with Internet addresses.

- Address mapping must be performed at each step along the path from the original source to the destination. The sender must map the intermediate router's Internet address to a physical address. The problem of mapping high-level addresses to physical addresses is known as the address resolution problem and has been solved in several ways. Physical addresses are two types.

  1. Ethernet 2. ProNET

- Ethernet has large and fixed physical addresses. ProNET has small, easily configured physical addresses. Address resolution is difficult for ethernet like networks but easy for network like porNET. ARP allows a host to find the physical address of a target host on the same physical network, given only the target's IP address.
- Fig. Q.22.1 (a) shows host A broadcasts an ARP request containing I_B to all computer on the network and Fig. Q.22.1 (b) shows host B responds with an ARP replay that contains the pair (I_B, P_B). To reduce communication costs, ARP maintain a cache of recently acquired IP to Physical address binding, so they do not have to use ARP repeatedly. Whenever a computer receives an ARP reply, it saves the sender's IP address and corresponding hardware address in its cache for successive lookups. When transmitting a packet, a computer always look in its cache for a binding before sending an ARP request. If a computer finds the desired binding in its ARP cache, it need not broadcast on the network. When ARP message travel from one computer to another, they must be carried in physical frame.
- Fig. Q.22.2 shows that the ARP message is carried in the data portion of a frame.
- To identify the frame as carrying on ARP message, sender assigns a special value to the type field in the frame header, and places the ARP message in the frame data field. The data in ARP packets does not have a fixed format header.

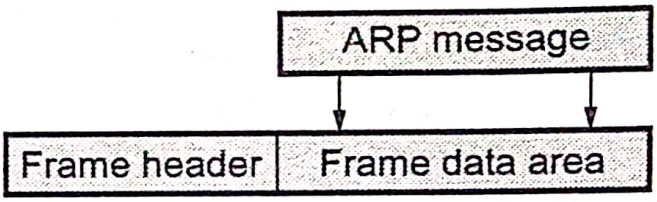


Fig. Q.22.2 An ARP message encapsulated in a physical network

Q.23 A host with IP address 130.23.3.20 and physical B 23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address A46EF45983AB. The two hosts are on the same Ethernet networt. Show the ARP request and reply packets encapsulated in Ethernet frames. ☞ [SPPU : May-19, End Sem, Marks 6]

Ans. : ARP request and reply packets is shown.

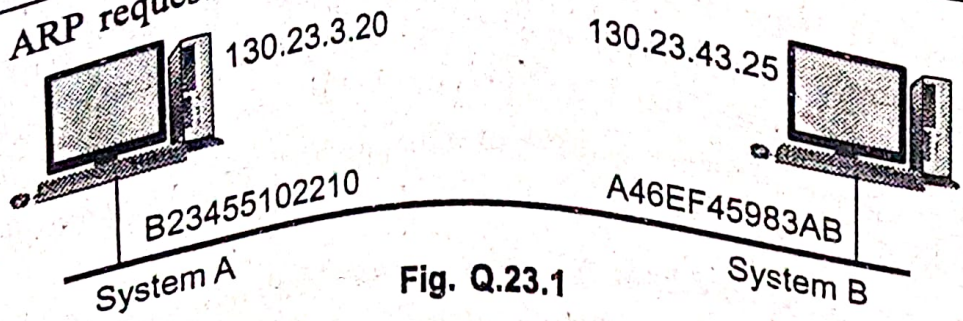


Fig. Q.23.1

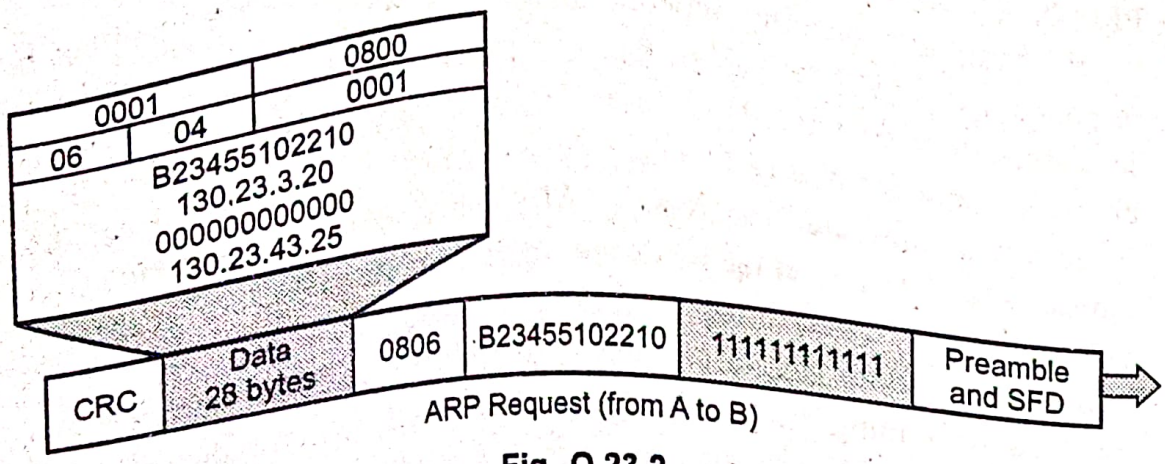


Fig. Q.23.2

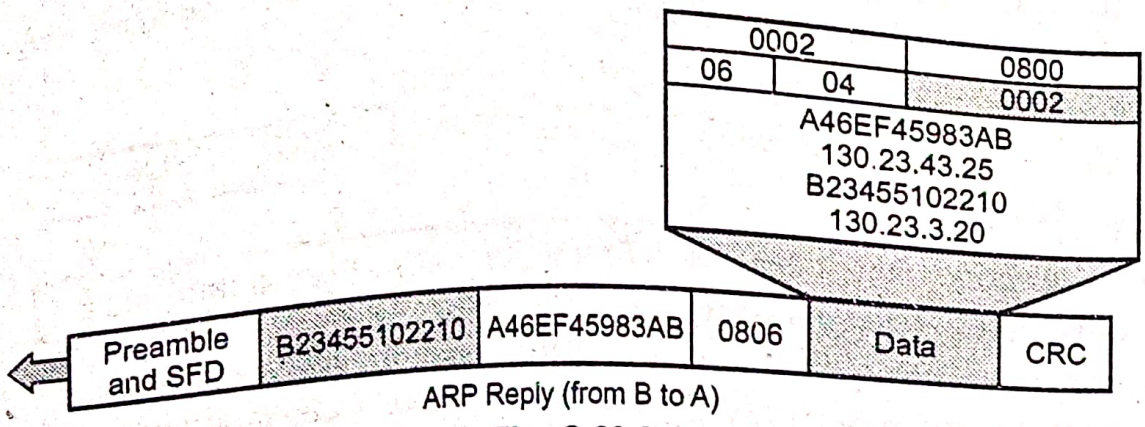


Fig. Q.23.3

The ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why the regular 4-byte boundaries for these addresses is not shown.

Hexadecimal for every field except the IP addresses is used.

Q.24 A host with IP address 130.23.3.20 and physical address B23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address A46EF45983AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames. ☞ **[Dec.-17, End Sem, Marks 4]**

Ans. : Refer Fig. Q.24.1 on next page.

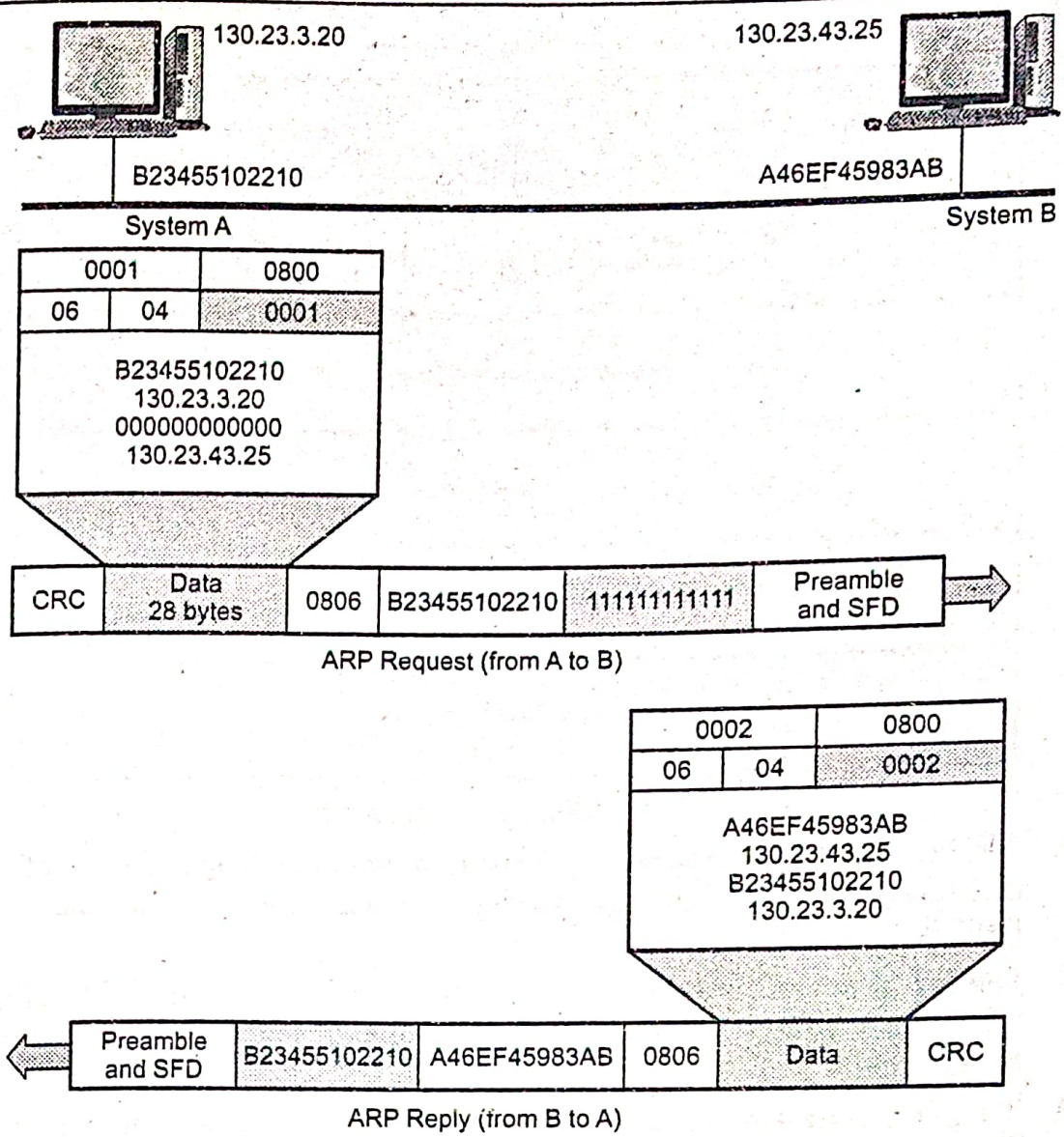


Fig. Q.24.1

Q.25 Explain ARP packet format.

Ans. : • Fig. Q.25.1 shows the ARP packet format.

1. **Hardware type :** This is 16 bits field defining the type of the network on which ARP is running. Ethernet is given the type 1.
2. **Protocol type :** This is 16 bits field defining the protocol. The value of this field for the IPv4 protocol is 0800H.
3. **Hardware length :** This is an 8 bits field defining the length of the physical address in bytes. Ethernet is the value 6.
4. **Protocol length :** This is an 8 bits field defining the length of the logical address in bytes. For the IPv4 protocol the value is 4.
5. **Opertion :** This is a 16 bits field defining the type of packet. Packet types are ARP request (1), ARP reply (2).

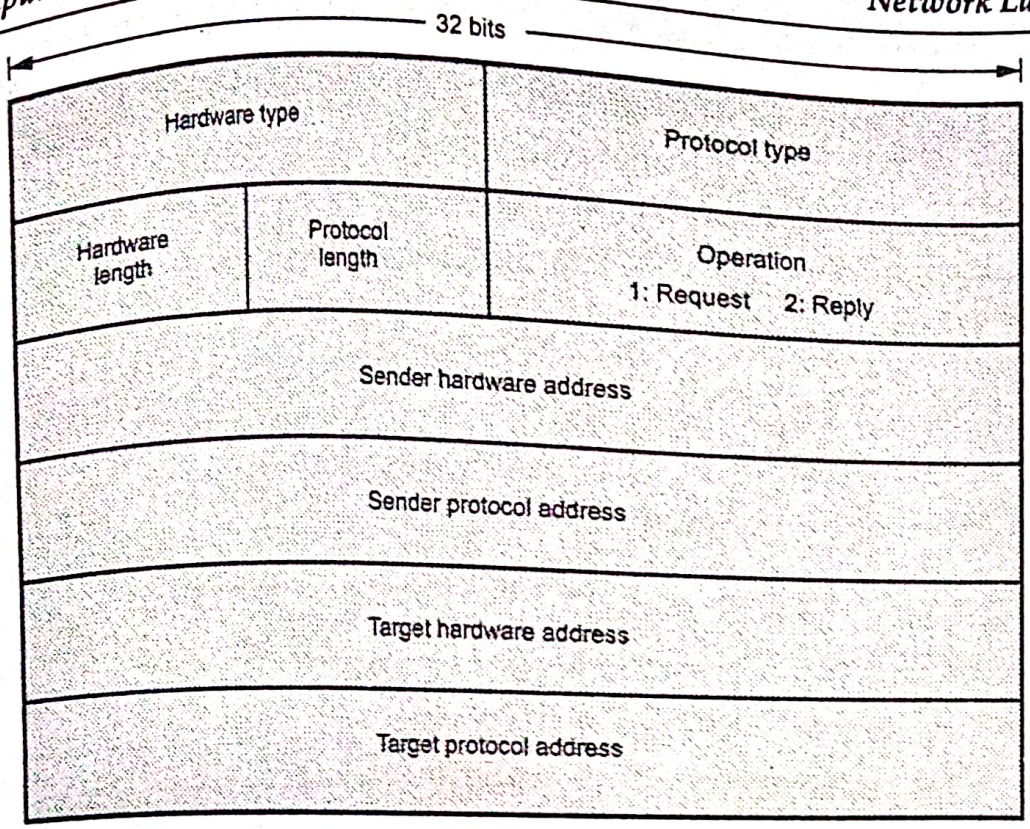


Fig. Q.25.1 ARP packet

6. **Sender hardware address :** This is a variable length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
7. **Sender protocol address :** This is also a variable length field defining the logical address of the sender. For the IP potocol, this field is 4 bytes long.
8. **Target hardware address :** This is a variable length field defining the physical address of the target. For Ethernet this field is 6 bytes long. For ARP request message, this field is all 0s because the sender does not know the physical address of the target.
9. **Target protocol address :** This is also a variable length field defining the logical address of the target. For the IPv4 protocol, this field is 4 bytes long.

Q.26 Write short note on RARP.

Ans. : • A diskless machine uses a TCP/IP Internet protocol called **RARP** to obtain its IP address from a server. RARP uses the same message format like ARP. RARP allows for multiple physical network types.

• RARP message is sent from one computer to another encapsulated in the data portion of a network frame. Fig. Q.26.1 shows the operation of RARP.

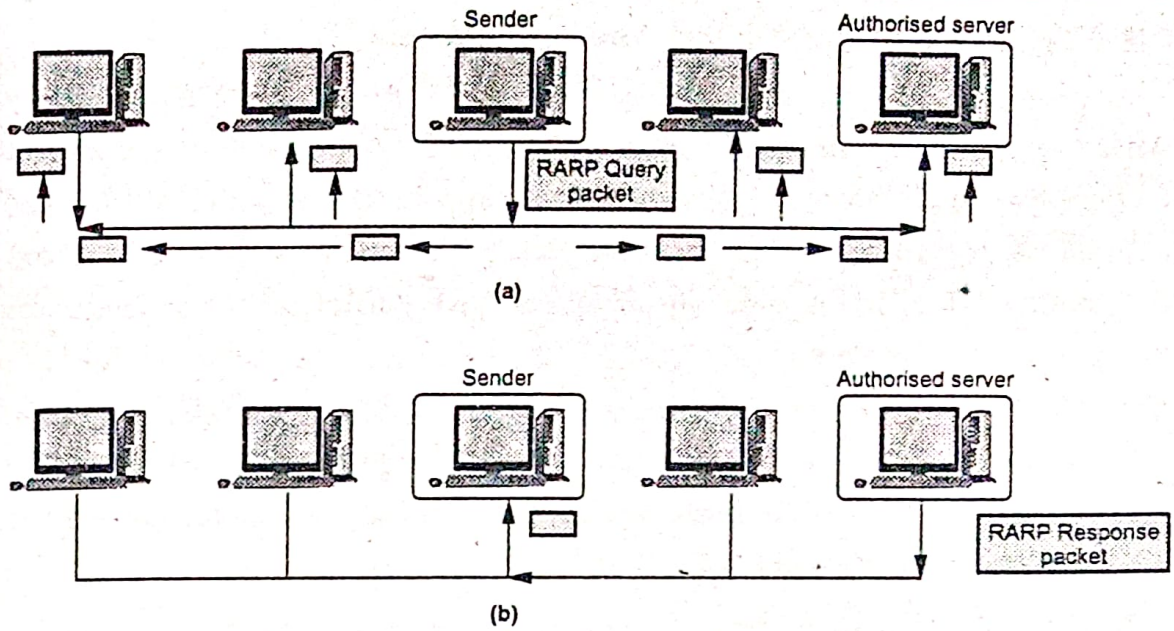


Fig. Q.26.1

- RARP perform following steps to obtain an IP address from the server.
  a) The sender broadcast the RARP request to all the other host present in the network.
  b) The RARP request packet contains the physical address of the sender.
  c) All the host receiving the RARP request packet process it but, the authorized host only which can serve RARP service, responds to the RARP request packet such host are known as **RARP server.**
  d) The authorized RARP server replies directly to requesting host with the RARP response packet which contains IP address for the sender.
- The RARP translates unique hardware addresses into Internet addresses on the Ethernet local area network (LAN) adapter.
- Standard Ethernet protocol is supported with the following restrictions :
  a) The server only replies to RARP requests.
  b) The server only uses permanent ARP table entries.
  c) The server does not use dynamic ARP table entries.
  d) The server does not automatically reply for itself.

Q.27 Write short note on ICMP.

☞ [SPPU : Dec.-17, May-19, End-Sem, Marks 6]

OR Explain : Internet Control Message Protocol (ICMP).

☞ [SPPU : May-18, Dec.-19, End-Sem, Marks 4]

Ans. : • There are some situations in which IP cannot deliver the packet to the destination host. For instance, this happens if the packet's TTL has expired, if the route to the specified destination address is missing from the routing table, if the gateway does not have sufficient buffer space for passing specific packet.

- It was noted earlier that if a router could not forward a packet for some reasons, the router would send an error message back ot the source to report the problem. The **Internet Control Message Protocol (ICMP)** is the protocol that handles error and other control messages.
- ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Although ICMP messages are encapsulated by IP packets.
- The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.
- All ICMP messages fall in the following classes :

  1. Error reporting 2. Query.

- The error reporting messages report problems that a router or a host may encounter when it processes an IP packet.
- The query messages, which occurs in pairs, help a host or a network manager get specific information from a router or another host.
- ICMP used by both hosts and gateway for a variety of functions, and especially by network management. The main functions associated with the ICMP are as follows :

  1. Error reporting 2. Reachability testing
  3. Congestion control 4. Route change notification
  5. Performance measuring 6. Subnet addressing.

- ICMP is used for error messages such as occur when something is detectably wrong with the packet format, with the selection of a route or with the condition of some intermediate node in the internet. Such

abnormal conditions are reported to the source of the datagram for possible **remedial** action.

For example, if user attempt to connect to a host, the user's system may get back an ICMP message saying "host unreachable". ICMP can also be used to find out some information about the network.

ICMP is similar to UDP in that it handles messages that fit in one datagram. It is simpler than UDP. It does not even have port numbers in the header. Since all ICMP messages are interpreted by the network software itself, no port number is needed to say where an ICMP message is supported to go. ICMP also provides a way for new nodes to discover the subnet mask currently used in an internetwork. So ICMP is an integral part of any IP implementation, particularly those that run in routers.

.28 Explain ICMPs echo request and reply.

ns. : • This query message is used for diagnostic purposes. Network anager and users utilize this pair of messages to identify network oblems. The echo request and echo reply test the communication path om a sender to a destination.

A host or router can send an echo request message to another host or router. The host or router that receives an echo request message creates an echo reply message and returns it to the original sender.

The echo request and echo reply messages can be used to determine if there is communication at the IP level. Because the ICMP messages are encapsulated in IP datagram's.

An echo request message can be sent by a host or router. An echo reply message is sent by the host or router which receives an echo request message.

Echo request and echo reply messages can be used by network managers to check the operation of the IP protocol. If a router returns a reply, then it and IP are working.

Echo request and echo reply messages can test the reachability of a host. This is usually done by invoking the ping command. The node to be tested is sent an echo request message. The optional data field

contains a message that must be repeated exactly by the respondin node in its echo reply message.

- Fig. Q.28.1 shows the format of the echo request and echo reply messages.

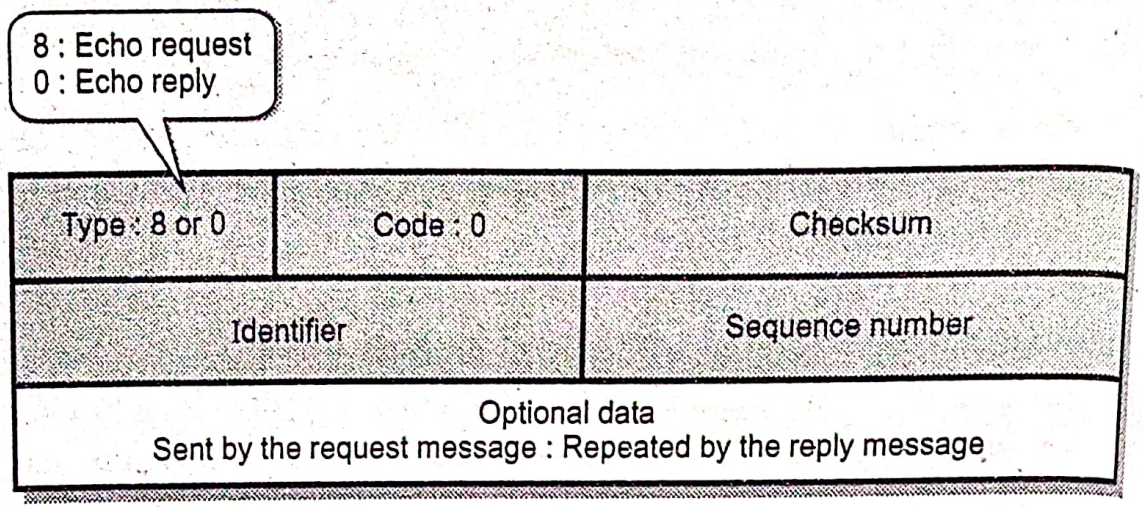


Fig. Q.28.1 Format of the echo request and echo reply messages

- Identifier field and sequence number field are not used and can be arbitrarily set by the sender. Identifier field is often the same as the process ID.

Q.29 Write short note on Internet Group Management Protocol (IGMP).

Ans. : • IGMP is a network layer protocol used to establish membership in a multicast group and can register a router to receive specific Multicast traffic.

- IGMP runs between a router and a node that enables the following actions :
  a) Routers ask nodes if they need a particular multicast stream (IGMP query).
  b) Nodes respond to the router if they are seeking a particular multicast stream (IGMP reports).
- IGMP uses IP addresses that are set aside for multicasting. Multicast IP addresses are in the range between 224.0.0.0 and 239.255.255.255.
- Each multicast group shares one of these IP addresses. When a router receives a series of packets directed at the shared IP address, it will

duplicate those packets, sending copies to all members of the multicast group.

- IGMP multicast groups can change at any time. A device can send an IGMP "join group" or "leave group" message at any point.
- IGMP works directly on top of the Internet Protocol (IP). Each IGMP packet has both an IGMP header and an IP header.
- A routing device receives explicit join and prune messages from those neighboring routing devices that have downstream group members. When Protocol Independent Multicast (PIM) is the multicast protocol in use, IGMP begins the process as follows :

1. To join a multicast group (G), a host conveys its membership information through IGMP.
2. The routing device then forwards data packets addressed to a multicast group G to only those interfaces on which explicit join messages have been received.
3. A designated router (DR) sends periodic join and prune messages toward a group-specific rendezvous point (RP) for each group for which it has active members. One or more routing devices are automatically or statically designated as the RP, and all routing devices must explicitly join through the RP.
4. Each routing device along the path toward the RP builds a wildcard (any-source) state for the group and sends join and prune messages toward the RP.

IGMP messages :

1. Membership reports : Devices send these to a multicast router in order to become a member of a multicast group.
2. "Leave group" messages : These messages go from a device to a router and allow devices to leave a multicast group.
3. General membership queries : A multicast-capable router sends out these messages to the entire connected network of devices to update multicast group membership for all groups on the network.
4. Group-specific membership queries : Routers send these messages to a specific multicast group, instead of the entire network.

3.6 : Network Routing and Algorithms

Q.30 What is routing ? How routing works ? Explain properties of routing algorithm.

Ans. : • In networking, routing is the process of moving a packet of data from source to destination. Routing is the process of path selection in any network.

- When a router receives a packet, it reads the headers of the packet to see its intended destination. It then determines where to route the packet based on information in its routing table.
- As a packet travels to its destination, it may be routed multiple times by several routers. Routers perform this process millions of times a second with millions of packets.

Properties of routing algorithm

Certain properties which are desirable in a routing algorithm are -

Correctness, simplicity, robustness, stability, fairness, optimality and efficiency.

1. Correctness and simplicity are self-explanatory.
2. Robustness means the ability to cope with changes in the topology and traffic without requiring all jobs in hosts to be aborted and network to be rebooted everytime.
3. Stability refers to equilibrium state of algorithm. It is the technique that react to changing conditions such as congestions. Under any conditions the network must not react too slow or experience unstable swings from one extreme to another.

Q.31 Explain static and dynamic routing algorithm.

Ans. : Routing algorithm can be classified in several ways. Based on their responsiveness it can be classified into two types -

1. Static (non-adaptive) Routing Algorithms.
2. Dynamic (adaptive) Routing Algorithms.

1. Static (non-adaptive) routing algorithms

- In static routing the network topology determines the initial paths. The precalculated paths are then loaded to the routing table and are fixed for

a longer period. Static routing is suitable for small networks. Static routing becomes **cumber some** for bigger networks.

- The disadvantage of static routing is its inability to respond quickly to network failure.

2. Dynamic (Adaptive) routing algorithms

- Dynamic routing algorithms change their routing decision if there is change in topology, traffic. Each router continuously checks the network status by communicating with neighbours. Thus a change in network topology is eventually propagated to all the routers. Based on this information gathered, each router computes the suitable path to the destination.
- The disadvantage of dynamic routing is its complexity in the router.

Q.32 Discuss difference between static and dynamic routing.

Ans. :

Sr. No.	Static routing (Non adaptive)	Dynamic routing (Adaptive)
1.	Static routing manually sets up the optimal paths between the source and the destination computers.	Dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.
2.	The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths.	The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network.
3.	These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network.	The dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination.

4.	The static routing is suitable for very small networks and they cannot be used in large networks	Dynamic routing is used for larger networks.
5.	The static routing is the simplest way of routing the data packets from a source to a destination in a network.	The dynamic routing uses complex algorithms for routing the data packets.
6.	The static routing has the advantage that it requires minimal memory.	Dynamic routers have quite a few memory overheads, depending on the routing algorithms used.
7.	The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing.	In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

3.7 : Distance Vector Routing

Q.33 Explain distance vector routing.

☞ [SPPU : Dec.-18, End Sem, Marks 6]

Ans. : Distance vector routing :

- Distance vector routing algorithm is the dynamic routing algorithm. It was designed mainly for small network topologies.
- Distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm.
- The term distance vector derives from the fact that the protocol includes its routing updates with a vector of distances or hop counts.

- In this algorithm, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts :
  a. The preferred outgoing line to use for that destination.
  b. An estimate of the time or distance to that destination.
- The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, etc.
- Assume that delay is used as a metric and that the router knows the delay to each of its neighbours. All nodes exchange information only with their neighbouring nodes.
- Nodes participating in the same local network are considered neighbouring nodes.
- Once every 'T' msec each router sends to each neighbour a list of its estimated delays to each destination. It also receives a similar list from each neighbour.
- By performing calculation for each neighbour, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table. Old routing table is not used in the calculation.
- Fig. Q.33.1 shows the subnet with 12 routers.

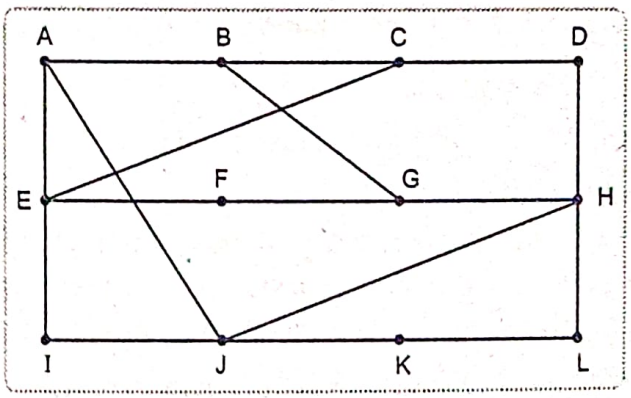


Fig. Q.33.1 Subnet

- Routing table for the subnet is shown below.

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6		New routing table for J

Vectors received from J's four neighbours

Advantages of Distance Vector routing :

1. It is simpler to configure than Link State.
2. It is simpler to maintain than Link State.
3. It requires low resource requirements (memory, CPU).

Disadvantages of Distance Vector routing :

1. It is slower to converge than Link State.
2. It is at risk from the count-to-infinity problem.
3. It creates more traffic than Link State since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
4. For larger networks, Distance Vector routing results in larger routing tables than Link State since each router must know about all other routers. This can also lead to congestion on WAN links. RIP announces host or default routes by default.
5. Limited scalability.

Q.34 Consider the subnet in Fig. Q.34.1. Distance vector routing is used and the following vectors have just come in to router C : from B (5, 0, 8, 12, 6, 2) ; from D (16, 12, 06, 0, 9, 10); and from E (7, 6, 3, 9, 0, 4). The measured delays to B, D and E are 6, 3 and 5 repectively. What is C's new routing table ? Give both the outgoing line to used and the expected delay ? ☞ [SPPU : May-19, End Sem, Marks 6]

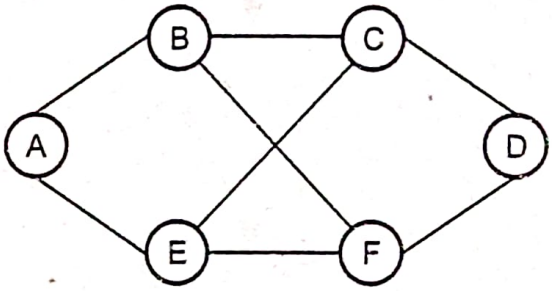


Fig. Q.34.1

Ans. : The distance table at C is So the routing table is -

	B	D	E
A	11	19	12
B	6	15	11
D	18	3	14
E	12	12	5
F	8	13	9

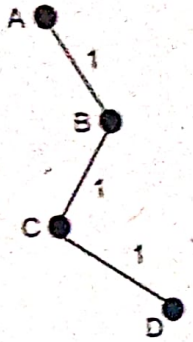
	Dist, Next hop
A	11, B
B	6, B
D	3, D
E	5, E
F	8, B

Q.35 Explain count-to-infinity problem.

☞ [SPPU : Dec.-19, End Sem, Marks 6]

Ans. : • Fig. Q.35.1 shows an imagined network and denotes the distances from router A to every other router. Until now everything works fine.

- Suppose that link (A, B) is broken. Router B observed it, but in his routing table he sees, that router C has a route to A with 2 hops. The problem is, that B does not know that C has router B as successor in his routing table on the route to A. That followed **count-to-infinity** problem. Router B actualizes his routing table and takes the router to A over router C.



Routing table for A

B	C	D
1	2	3

Fig. Q.35.1

B	C	D
3	2	3

B	C	D
3	4	3

B	C	D
5	4	5

Fig. Q.35.2

- In Fig. Q.35.2, we can see the new distances to A. In router C's routing the route to A contains router B as next hop router, so if B has increased his costs to A, C is forced to do so. Router C increases his cost to A about B ÷ 1 = 4.
- Now we see the conseuqence of the distributed Bellman-Ford protocal : Because router B takes the path over C to A, he reactualizes his routing table and so on.
- There are several partial solutions to the count-to-infinity problem. The first one is to use some relatively small number as an approximation of infinity. For example, we might decide that the maximum number of hops to get across a certain network is never going to be more than 16 and so we could pick 16 as the value that represents infinity.
- This at least bounds the amount of time that it takes to count to infinity. Of course, it could also present a problem if our network grew to a point where some nodes were separated by more than 16 hops.
- One technique to improve the time to stabilize routing is called **split horizon**. Split horizon technique implies that routing information about some network stored in the routing table of a specific router is never sent to the router from which it was received.

3.8 : Link State Routing

Q.36 Explain link state routing algorithm with example.

☞ [SPPU : May-17,18, End Sem, Marks 4]

Ans. : Link State Routing

- Link state routing is the second major class of intradomain routing protocol. It is **dynamic** type routing algorithm.
- The idea behind link state routing is simple and can be stated as five parts. Each router must do the following :

1. **Learning about the neighbors :** When a router is booted, it sends a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is. When two or more routers are connected by a LAN, the LAN can be modeled as a node.
2. **Measuring line cost :** To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. Should the load be taken into account when measuring the delay ?
3. **Building link state packets :** State packets may be built periodically, or when some significant event occurs, such as a line or neighbor going down or coming back up again.
4. **Distributing the link state packets :**

- Each state packet contains a sequence number that is incremented for each new packet sent.
- Routers keep track of all the (source router, sequence) pairs they see.
- When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on (i.e., flooding). If it is a duplicate, it is discarded. If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete.

4.	Send small updates everywhere.	Sends larger updates only to neighbouring routers.
5.	Require more CPU power and more memory space.	Require less CPU power and less memory space.
6.	Protocol example - OSPF and BGP.	Protocol example - RIP

3.9 : Routing Protocols : RIP, OSPF, BGP

Q.38 Draw the packet header format of OSPF and explain in detail.

☞ [SPPU : Dec.-15, Marks 8]

Ans. : OSPF :

- OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map, which is regularly updated.
- Each node contains a routing directory database. This database contains information about the routers interfaces that are operable, as well as status information about adjacent routers. This information is periodically broadcast to all routers in the same domain.

SPF Header Format

The header format for OSPF is shown in the Fig. Q.38.1.

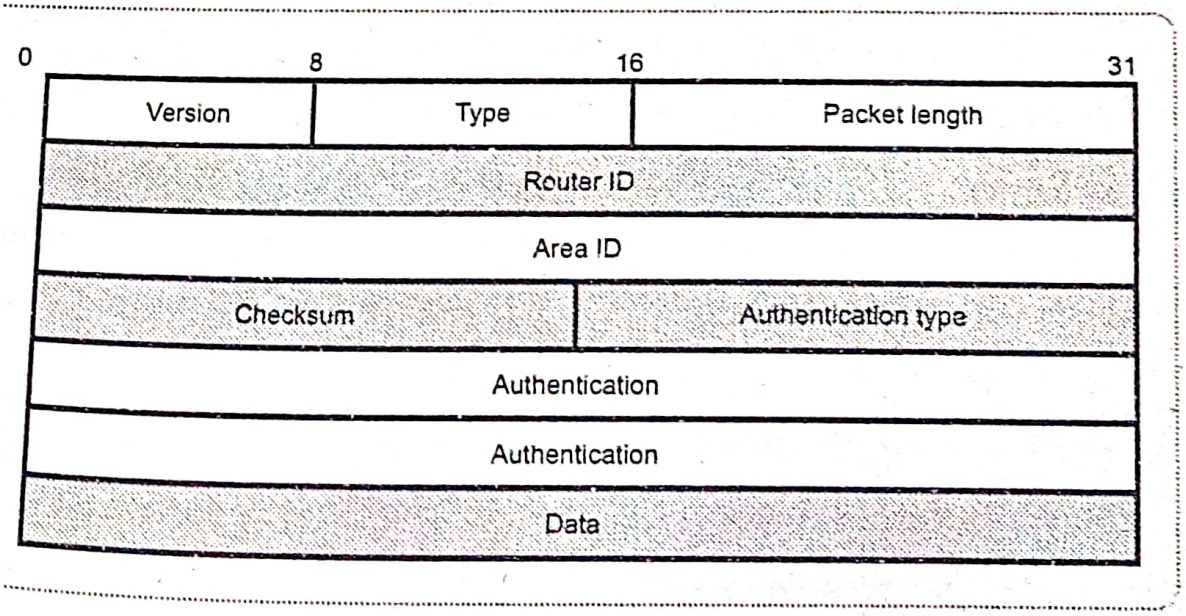


Fig. Q.38.1 OSPF header format

Problems with the basic algorithm :

1. The sequence numbers may wrap around, causing confusion. Solution : using a 32-bit sequence number. With one packet per second, it would take 137 years to wrap around.
2. If a router ever crashes, it will lose track of its own sequence number. If it starts again at the sequence number 0, new packets will be rejected as obsolete/duplicate by other routers.
3. If a sequence number is ever corrupted and 65,540 is received instead of 4 (a 1-bit error), packets 5-65540 will be rejected as obsolete.

5. **Computing the new routes :** Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph. Then Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

- Link state routing protocols use event driven updates rather than periodic updates. Link state routing is widely used in actual networks. OSPF protocol uses in a link state algorithm.
- Link state routing protocols are as follows :
  a. Open Shortest Path First (OSPF)
  b. Network Link Services Protocol (NLSP).
  c. Apple's AURP.
  d. ISO's Intermediate System-Intemediate System (IS-IS).

Q.37 Compare link state routing and distance vector routing.

☞ [SPPU : Dec.-15, Marks 6]

Ans. : Comparison of Link state routing and Distance vector routing

Sr. no.	Link State Routing	Distance Vector Routing
1.	Dijkstra's algorithm used to calculate link state cost.	Bellman-ford algorithm used to calculate the shortest cost path.
2.	Sends message to every other node in the network.	Sends message to their neighbours.
3.	It is centralized global routing algorithm.	It is decentralized routing algorithm.

4.	Send small updates everywhere.	Sends larger updates only to neighbouring routers.
5.	Require more CPU power and more memory space.	Require less CPU power and less memory space.
6.	Protocol example - OSPF and BGP.	Protocol example - RIP

3.9 : Routing Protocols : RIP, OSPF, BGP

Q.38 Draw the packet header format of OSPF and explain in detail.

☞ [SPPU : Dec.-15, Marks 8]

Ans. : OSPF :

- OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map, which is regularly updated.
- Each node contains a routing directory database. This database contains information about the routers interfaces that are operable, as well as status information about adjacent routers. This information is periodically broadcast to all routers in the same domain.

SPF Header Format

The header format for OSPF is shown in the Fig. Q.38.1.

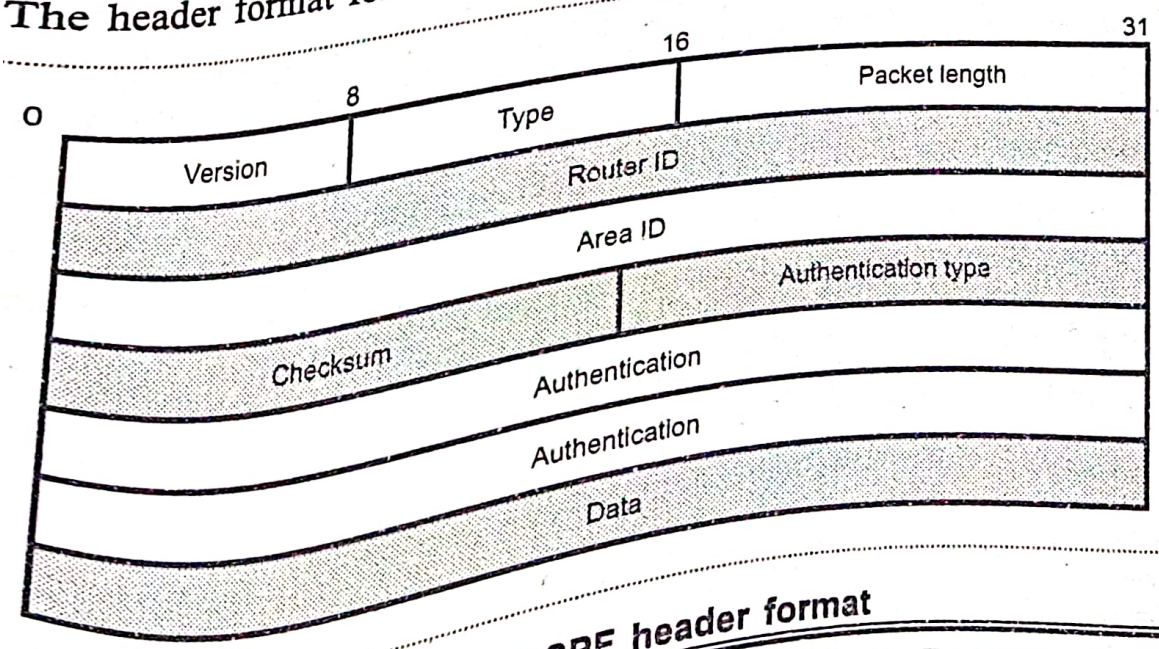


Fig. Q.38.1 OSPF header format

- Details of OSPF header format :

1. **Version :** This field specifies the protocol version.
2. **Type :** This field indicates messages as one of the following type.
   a. Hello b. Database description
   c. Link status d. Link status update
   e. Link status acknowledgement
3. **Packet length :** This field specifies the length of OSPF packet in bytes, including the OSPF header.
4. **Router ID :** It identifies the sending router. This field is typically set to the IP address of one of its interfaces.
5. **Area ID :** This field identifies the area this packet belongs to (Transmitted).
6. **Checksum :** The checksum field is used to detect errors in the packet. The checksum is performed on the entire packet.
7. **Authentication type :** It identifies the authentication type that is used.
8. **Authentication :** This field includes a value from the authentication type.

Q.39 Explain BGP routing protocol. ☞ [SPPU : Dec.-16, Marks 4]

Ans. : • The purpose of an exterior gateway protocol is to enable two different Autonomous System (AS) to exchange routing information so that IP traffic can flow across the autonomous system border.

- The BGP is an interdomain routing protocol that is used to exchange network reachability information among BGP routers (Also called BGP speakers). Each BGP speaker establishes a TCP connection with one or more BGP speakers (routers).
- Two routers are considered to be neighbours if they are attached to the same subnetwork. If the two routers are in different autonomous systems, they may wish to exchange routing information.
- BGP performs three functional procedures.
  1. Neighbour acquisition
  2. Neighbour reachability
  3. Network reachability

- Neighbour acquisition procedu information between two router To perform neighbor acquisitic another. If the target router a message in response.
- Once a neighbour relationship procedure is used to maintai assured that the other side neighbour relationship. For messages to each other. Bot subnetworks that it can reac subnetwork.
- If the database changes, broadcast to all other route these update message, all routing information.
- BGP connections inside a (iBGP) and BGP connecti called external BGP (eBG
- Fig. Q.39.1 shows the int

Fig.

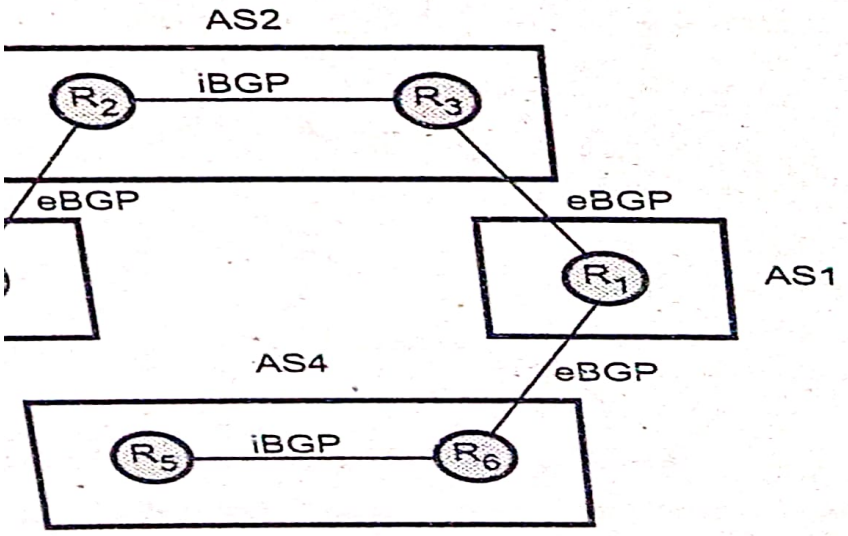
dures used for exchanging the routing
ers in different Autonomous Systems (AS).
ion, one router sends an open message to
accepts the request, it returns a keepalive

ip is established, the neighbour reachability
ain the relationship. Both sides needs to be
le still exists and is still engaged in the
this purpose, both routers send keepalive
oth sides router maintains a database of the
ach and the perferred route for reaching that

, router issues an update message that is
ers implementing BGP. By the broadcasting of
l the BGP routers can build up and maintain

an autonomous system are called internal BGP
ctions between different autonomous systems are
BGP).

nternal and external BGP.



. Q.39.1 Internal and external BGP

Q.40 Explain RIP with example.

Ans. : • In RIP, routing updates are exchanged between neighbours approximately every 30 seconds using a so-called **RIP response message.** The response message sent by a router or host contains a list of upto 25 destination networks within an autonomous system (AS). Response messages are also known as **RIP advertisements.**

• Fig. Q.40.1 shows a portion of an autonomous system.

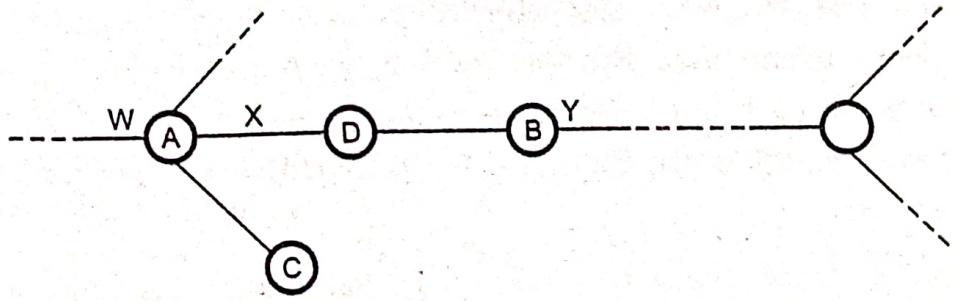


Fig. Q.40.1 Portion of AS

• Forwarding table in router D before receiving advertisement from router A. For this example, the table indicates that to send a datagram from router D to destination network W, the datagram should first be forwarded to neighbouring router A; the table also indicates that destination network W is two hops away along the shortest path.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	B	7
X	–	1
.....	.....	.....

Table Q.40.1 Forwarding table

• The Table Q.40.1 also indicates that network Z is seven hops away via router B.

- Now suppose that 30 seconds later, router D receives from router A the advertisement shown in Table Q.40.2.

Destination network	Next router	Number of hops to destination
Z	C	4
W	–	1
X	–	1
.....	.....	.....

Table Q.40.2 Advertisement from router A

- Note that the advertisement is nothing other than the forwarding table information from router A. This information indicates, in particular, that network Z is only four hops away from router A. Router D, upon receiving this advertisement, merges the advertisement with the old routing table.
- Router D learns that there is now a path through router A to network Z that is shorter than the path through router B. Thus, router D updates its forwarding table to account for the shorter shortest path, as shown in Table Q.40.3.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	A	3
.....	.....	.....

Table Q.40.3

- RIP routers exchange advertisements approximately every 30 seconds. If a router does not hear from its neighbour atleast once every 180 seconds, that neighbour is considered to be no longer reachable; i.e. either the neighbour has died or the connecting link has gone down. When this happens, RIP modifies the local forwarding table and then

propagates this information by sending advertisements to its neighbouring routers.

- A router can also request information about its neighbour's cost to a given destination using RIP's request message. Routers send RIP request and response messages to each other over UDP using port number 520.

Q.41 Explain difference between RIP and OSPF.

Ans. :

Sr. No.	RIP	OSPF
1.	RIP is easy to configure.	OSPF is complicated to configure and requires network design and planning.
2.	An end system (a system with only one network interface) can run RIP in passive mode to listen for routing information.	OSPF does not have a passive mode.
3.	RIP may be slow to adjust for link failures.	OSPF is quick to adjust for link failures.
4.	RIP generates more protocol traffic than OSPF.	OSPF generates less protocol traffic than RIP.
5.	RIP is not well suited to large networks, because RIP packet size increases as the number of networks increases.	OSPF works well in large networks.
6.	RIP is distance vector routing protocol.	OSPF is link state routing protocol.

3.10 : Routing in MANET

Q.42 Explain with example Ad-hoc on demand distance vector protocol.

Ans. : • AODV is a reactive MANET routing protocol means it discovers a route to destination only when it is required.

- AODV routing algorithm is similar to the distance vector algorithm that has been adapted to work in a mobile environment.
- In AODV, routes to destination host are discovered on demand i.e. it determines a route to some destination only when any node wants to send a packet to that destination.
- Two nodes are said to be connected if they can communicate directly by using their radios signals.
- The AODV routing algorithm maintains a routing table at each node.
- Consider the ad hoc network shown in Fig. Q.42.1 (a), in which a node 1 wants to send a packet to node 9.
- Suppose that node 1 checks in its routing table and does not find an entry for destination node 9. Now it is necessary to discover a route of node 9. This property of discovering routes only when they are needed is called as "on demand."
- To find node 9, node 1 constructs a special ROUTE REQUEST packet and broadcasts it using flooding.
- The packet reaches to node 2 and 4, as shown in the Fig. Q.42.1 (b).
- After receiving request from node 1, node 2 and 4 rebroadcast the request.
- This process of rebroadcasting continues to reach nodes 3, 6 and 7 as shown in Fig. Q.42.1 (c) and nodes 5, 8 and 9 in Fig. Q.42.1 (d).
- A sequence number is set at the source node to delete the duplicate entries during the flooding.
- For example, node 4 discards the transmission form node 2 in Fig. Q.42.1 (c) because it has already forwarded the request.

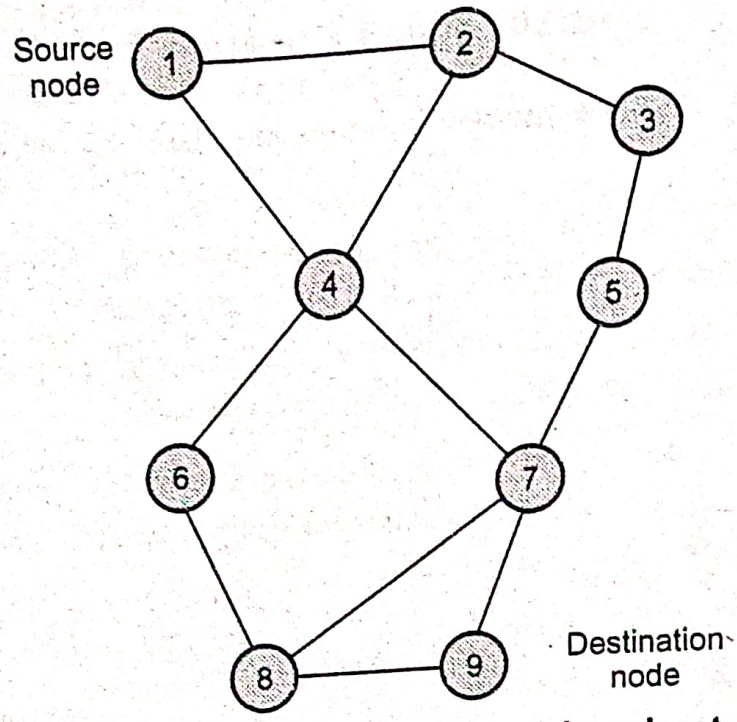


Fig. Q.42.1 (a) Adhoc network - Node 1 broadcast packet

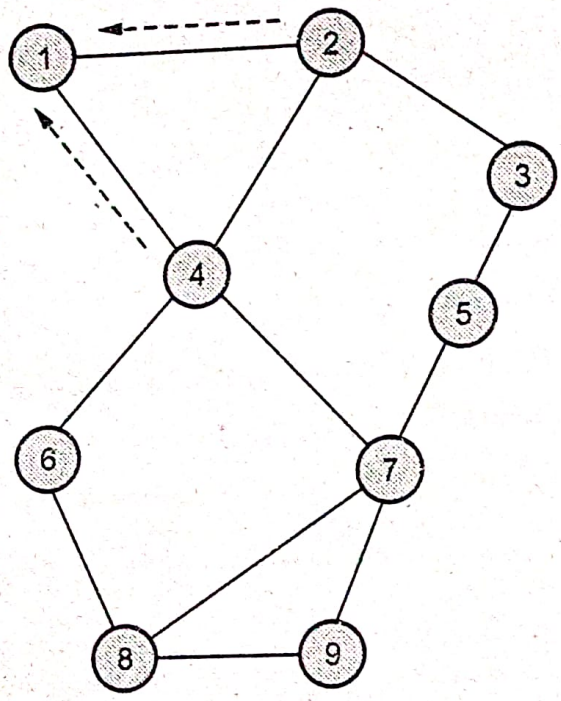


Fig. Q.42.1 (b) After Node 2 and 4 have received node 1's broadcas

- Finally, the request reaches to node 9 and after receiving request pack from node 1, node 9 send a ROUTE REPLY packet to the sender. Th reply packet is a unicast packet sent by node 9.

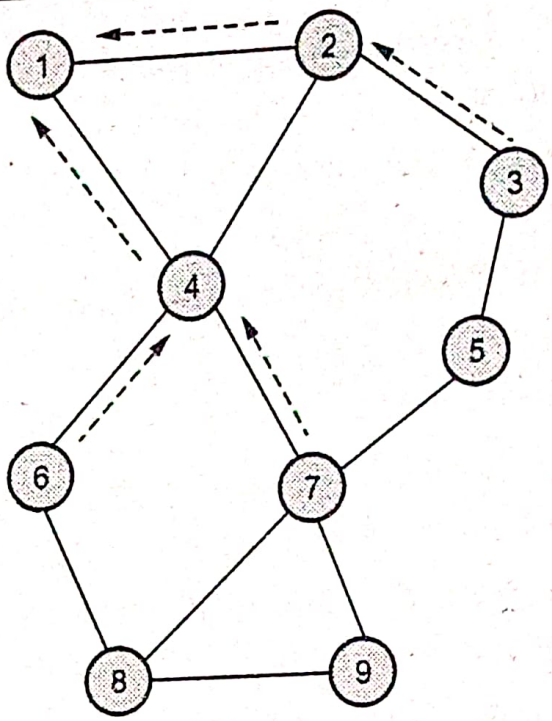


Fig. Q.42.1 (c) After node 3, 6, 7 have received 1's broadcast

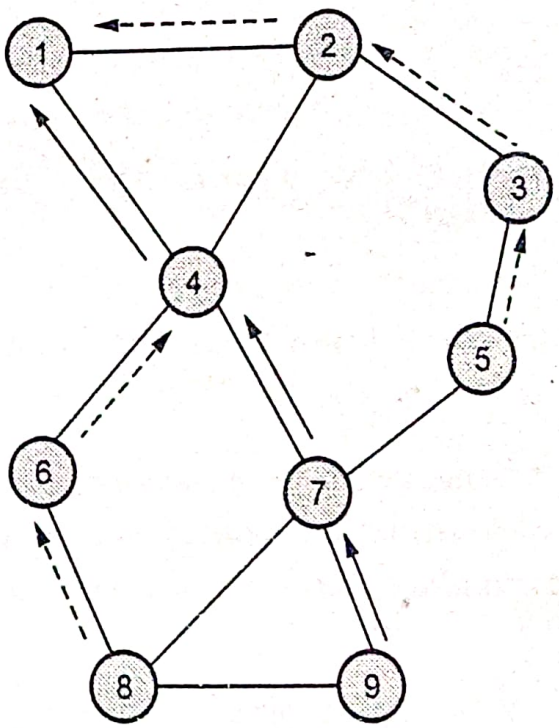


Fig. Q.42.1 (d) After node 5, 8 and 9 received 1's broadcast

- The arrows in Fig. Q.42.1 (b) - Fig. Q.42.1 (d) show the reverse route information that is stored during transmission.
- Each intermediate node also increments a hop count as it forwards the reply message.

- This information is important because it tells the nodes how far they are from the destination node.
- The replies tell each intermediate node which neighbor to use to reach the destination node.
- Intermediate nodes 7 and 4 are the best route stored in the routing table.
- When reply reaches node 1, a new route 1-4-7-9 has been created.
- In large network, the algorithm creates many broadcast packets even though the destination node is very close to the sender.
- So, to reduce overhead, the scope of the broadcast packets should be limited and it will be achieve using TTL field of IP packet.
- Hence, to find a destination host, the sender broadcasts a ROUTE REQUEST packet with TTL set to one.
- If no response comes back within a specified time, another packet is sent, this time TTL set to two. Subsequent attempts use 3, 4, 5, etc.

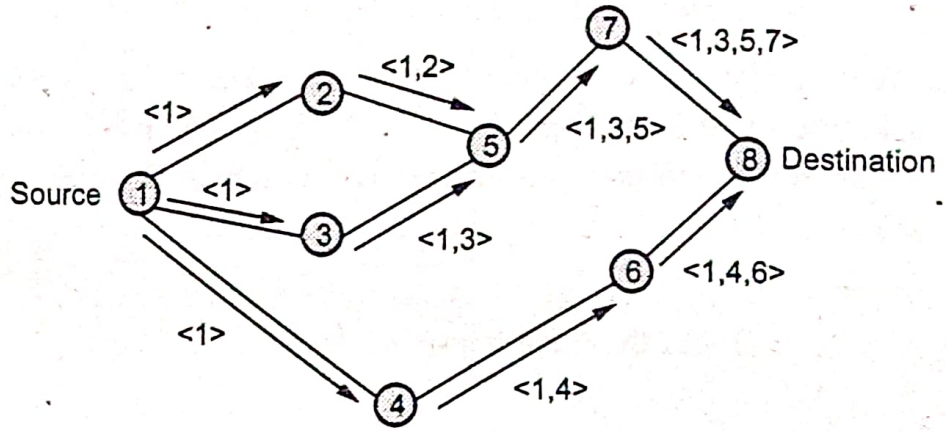
Q.43 How route discovery takes place in DSR ? Explain advantages and disadvantages of DSR.

Ans. : • The DSR protocol is composed of two mechanisms: route discovery and maintenance of source routes in the ad hoc network.

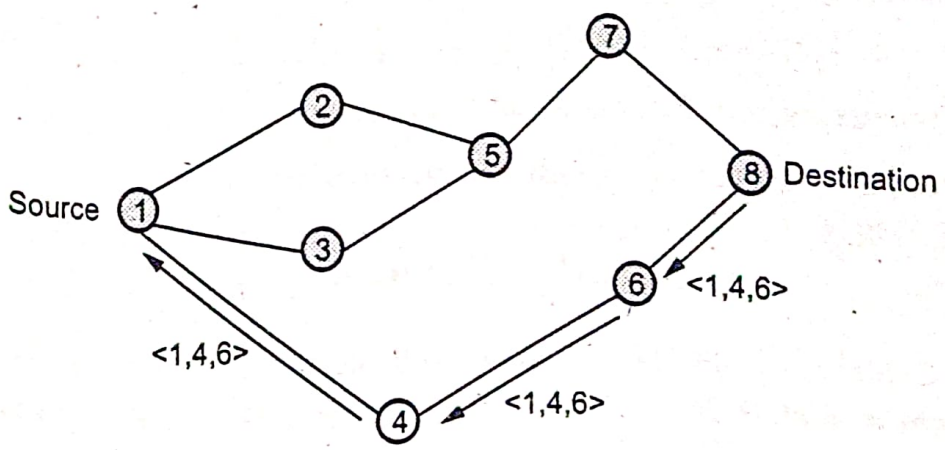
Route Discovery

- DSR uses source routing, rather than hop-by-hop routing. Thus, in DSR every packet header carries the ordered list of network nodes for routing. Thus, intermediate nodes do not need to maintain routing information.
- So, compare to AODV, the overhead is large in DSR because each packet must contain the whole sequence of nodes comprising the route. Therefore, DSR will be most efficient in small networks.
- If a source node wishing to set up a connection to another node, it initiates the route discovery process by broadcasting a ROUTE REQUEST packet. This packet is received by all neighboring nodes which then forward it to their own neighbors.

- After arrival of the ROUTE REQUEST message either to the destination or to an intermediate node that knows a route to the destination, the packet contains the sequence of nodes that constitute the route.
- This information is useful for piggybacking to the ROUTE REPLY message and made available at the source node.
- DSR supports both symmetric and asymmetric links. Therefore, the ROUTE REPLY message can be either carried over the same path with the original ROUTE REQUEST, or the destination node might creates its own route discovery towards the source node and piggyback the ROUTE REPLY message in its ROUTE REQUEST.
- This route discovery is shown schematically in following Fig. Q.43.1.



(a) Route request



(b) Route reply

Fig. Q.43.1 DSR route discovery

host number. For example, xxx.yyy.zzz.www in this xxx.yyy gives the class of IP and network number; the zzz.www is the host number. Routers all over the world have routing tables telling which line to use to get to network xxx.yyy. Whenever a packet comes in with a destination IP address of the form (xxx.yyy.zzz.www) it goes out on that line. If new IP address is configured to machine corresponding to its new location is unattractive because large number of users, programs and database would have to be informed of the change.

- Another approach is to have the routers use complete IP address for routing, instead of just the class and network. For this, each router requires millions of table entries.
- Following are some rules for using mobile IP.
  1. Each mobile host must be able to use its home IP address anywhere.
  2. Software changes to the fixed hosts were not permitted.
  3. Changes to the router software and tables were not permitted.
  4. No overhead should be incurred when a mobile host is at home.
- In mobile IP, every site that wants to allow its users to roam has to create a home agent and create foreign agent for visitors. When a packet arrives at the user's home local area network, it comes in at some router attached to the LAN. The router then tries to locate the host in the usual way, by broadcasting an ARP packet asking. The home agent responds to query by giving its own ethernet address. The router then sends packet for that address to the home agent. At the time the mobile host moves, the router probably has its ethernet address cached.
- To replace that ethernet address with the home agent's a trick called gratuitions ARP is used. Cryptographic authentication protocol are used for security.

END...

host number. For example, xxx.yyy.zzz.www in this xxx.yyy gives the class of IP and network number; the zzz.www is the host number. Routers all over the world have routing tables telling which line to use to get to network xxx.yyy. Whenever a packet comes in with a destination IP address of the form (xxx.yyy.zzz.www) it goes out on that line. If new IP address is configured to machine corresponding to its new location is unattractive because large number of users, programs and database would have to be informed of the change.

- Another approach is to have the routers use complete IP address for routing, instead of just the class and network. For this, each router requires millions of table entries.
- Following are some rules for using mobile IP.
  1. Each mobile host must be able to use its home IP address anywhere.
  2. Software changes to the fixed hosts were not permitted.
  3. Changes to the router software and tables were not permitted.
  4. No overhead should be incurred when a mobile host is at home.
- In mobile IP, every site that wants to allow its users to roam has to create a home agent and create foreign agent for visitors. When a packet arrives at the user's home local area network, it comes in at some router attached to the LAN. The router then tries to locate the host in the usual way, by broadcasting an ARP packet asking. The home agent responds to query by giving its own ethernet address. The router then sends packet for that address to the home agent. At the time the mobile host moves, the router probably has its ethernet address cached.
- To replace that ethernet address with the home agent's a trick called gratuitions ARP is used. Cryptographic authentication protocol are used for security.

END...

- In order to limit the overhead of this control messaging, each node maintains a route cache.
- Thus, all the possible routes that are determine are stored in the cache.
- The node updates entries in the route cache as and when it learns about new routes.
- Generally, Route maintenance is initiated by the source node upon detection of a change in network topology that prevents its packets from reaching the destination node.
- In such a case the source node can either attempt to use alternative routes to the destination node. Storing in the cache of alternative routes means that route discovery can be avoided when alternative routes for the broken one exist in the cache. Therefore route recovery in DSR can be faster than in other on-demand protocols.
- Since route maintenance is initiated only upon link failure, DSR does not make use of periodic transmissions of routing information, resulting in less control signaling overhead and less power consumption at the mobile nodes.

Advantages :

- Route cache improves the performance of the protocol.
- Faster routing possible for real time application having low to-end delay.

Disadvantages

- Route maintenance mechanism does not locally repair a broken link.
- Stale route cache information can result in delays.
- Performance degrades in highly mobile environments.

3.11 : Mobile IP

Q.44 Explain mobile IP protocol and describe triangular routing problem in mobile IP. ☞ [SPPU : Dec.-16, Marks 6]

Ans. : • IP addressing system makes working easier than mobile IP. Every IP address contains three fields. The class, the network number and

host number. For example, xxx.yyy.zzz.www in this xxx.yyy gives the class of IP and network number; the zzz.www is the host number. Routers all over the world have routing tables telling which line to use to get to network xxx.yyy. Whenever a packet comes in with a destination IP address of the form (xxx.yyy.zzz.www) it goes out on that line. If new IP address is configured to machine corresponding to its new location is unattractive because large number of users, programs and database would have to be informed of the change.

- Another approach is to have the routers use complete IP address for routing, instead of just the class and network. For this, each router requires millions of table entries.
- Following are some rules for using mobile IP.
  1. Each mobile host must be able to use its home IP address anywhere.
  2. Software changes to the fixed hosts were not permitted.
  3. Changes to the router software and tables were not permitted.
  4. No overhead should be incurred when a mobile host is at home.
- In mobile IP, every site that wants to allow its users to roam has to create a home agent and create foreign agent for visitors. When a packet arrives at the user's home local area network, it comes in at some router attached to the LAN. The router then tries to locate the host in the usual way, by broadcasting an ARP packet asking. The home agent responds to query by giving its own ethernet address. The router then sends packet for that address to the home agent. At the time the mobile host moves, the router probably has its ethernet address cached.
- To replace that ethernet address with the home agent's a trick called gratuitions ARP is used. Cryptographic authentication protocol are used for security.

END...

Unit IV

4 Transport Layer

4.1 : Process to Process Delivery

Q.1 What are the duties of transport layer ? Explain how QoS is improved. [SPPU : May-15, Dec-15, Marks 6]

Ans. : Duties/ functions of transport layer :

1. This layer breaks messages into packets.
2. It performs error recovery if the lower layer are not adequately error free.
3. Function of flow control if not done adequately at the network layer.
4. Functions of multiplexing and demultiplexing sessions together.
5. This layer can be responsible for setting up and releasing connections across the network.

- A transport layer protocol provides for logical communication between application processes running on different hosts. The logical communication means that the communicating application processes are not physically connected to each other from the applications' viewpoint.

Quality of service

- The transport protocol entity should allow the transport service user to specify the quality of transmission service to be provided. Following are the transport layer quality of service parameters

1. Error and loss levels
2. Desired average and maximum delay
3. Throughput
4. Priority level
5. Resilience.

- The error and loss level measures the number of lost or garbled messages as a fraction of the total sent.

- The desired average and maximum delay measures the time between a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine.
- The throughput parameter measures the number of bytes of user data transferred per second, measured over some time interval.
- The priority level parameter provides a way for a transport user to indicate that some of its connection are more important than other ones. The high priority connections get serviced before the low priority ones.

Q.2 Explain process to process delivery.

Ans. : • The transport layer is the fourth layer in the OSI layered architecture. The transport layer is responsible for reliable data delivery. The upper-layer protocols depends heavily on the transport layer protocol. A high level of error recovery is also provided in this layer. This layer ensures, that packets are delivered error free, in sequence and with no losses or duplications.

- Data link layer is responsible for delivery of frames between two neighboring nodes over a link. So this is called node-to-node delivery. Network layer is responsible for host-to-host delivery i.e. delivery of datagrams between two hosts.
- Transport layer is responsible for process to process delivery i.e. the delivery of a packet, part of a message from one process to another.
- Client server paradigm is used for process to process communication. A process on the local machine (hot) called a client needs services from a process usually on the remote host called server. Fig. Q.2.1 shows types of data deliveries.
- Nowadays, operating system support multiuser and multiprogramming environments. A remote computer can run several server programs at the same time.
- The services that a transport protocol can provide are often constrained by the service model of the underlying network layer protocol. If network layer protocol cannot provide delay or bandwidth guarantee for 4 PDU's sent between hosts, then the transport layer protocol cannot

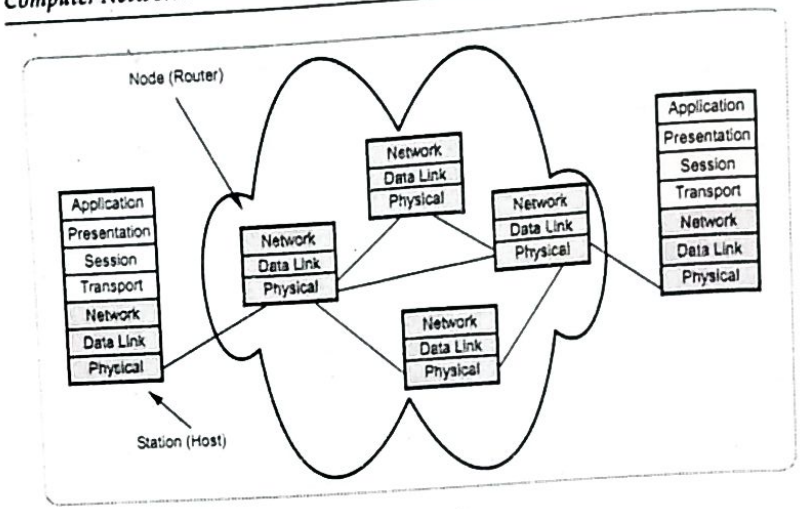


Fig. Q.2.1

provide delay or bandwidth guarantees for messages sent between processes.

- Some of the services offered by the transport protocol even when the underlying network protocol does not offer the corresponding service at the network layer.
- A transport protocol can offer reliable data transfer service to an application even when the underlying network protocol is unreliable, even when the network protocol loses, garbles and duplicate packets.

4.2 : Transport Service

Q.3 What are various transport service primitives ? Explain in brief.

☞ [SPPU : Dec.-13, Marks 4]

Ans. : Transport service primitives :

- To allow users to access the transport service, the transport layer must provide some operations to application programs. Real networks can lose packets, so the network service is generally unreliable. The transport service is reliable. Network service is used only by the transport entities. The transport service must be convenient and easy to use.

- Following are the primitives used for a simple transport service.

Primitive	Packet sent	Meaning
LISTEN	(None)	Block until some process tries to connect.
CONNECT	CONNECTION REQ	Actively attempt to establish a connection.
SEND	DATA	Send information.
RECEIVE	(None)	Block until a DATA packet arrives.
DISCONNECT	DISCONNECTION REQ	This side wants to release the connection.

- At the transport layer, even a simple unidirectional data exchange is more complicated than at the network layer. Every data packet sent will also be acknowledged. These acknowledgement are managed by the transport entities using the network layer protocol and are not visible to transport user.
- Transport Protocol Data Unit (TPDU) for messages sent from transport entity to transport entity. TPDU are contained in the packets. Packets are contained in frames. When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field up to the network entity. The network entity processes the packet header and passes the contents of the packet payload upto the transport entity.
- Fig. Q.3.1 shows the nesting of TPDU with packets.
- The client's CONNECT call causes a CONNECTION REQUEST TPDU to be sent to the server. When it arrives, the transport entity checks to see that the server is blocked on a LISTEN. It then unblocks the server and sends a CONNECTION ACCEPTED TPDU back to the client.

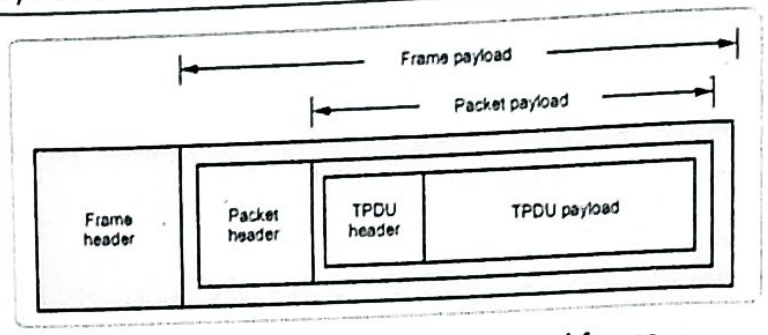


Fig. Q.3.1 Nesting of TPDU, packets and frames

When this TPDU arrives, the client is unblocked and the connection is established.

- Data can be exchanged using the SEND and RECEIVE primitives. When the TPDU arrives, the receiver is unblocked. It can then process the TPDU and send a reply.
- When a connection is no longer needed, it must be released to free up table space within the two transport entities. Disconnection has two types : Asymmetric and symmetric.

Q.4 Explain transport layer design issues.

Ans. : The transport layer delivers the message from one process to another process running on two different hosts. Thus, it has to perform number of functions to ensure the accurate delivery of message. The various functions of transport layer are :

1. Establishing, maintaining and releasing connection
   - The transport layer establishes, maintains and releases end-to-end transport connection on the request of upper layers.
   - Establishing a connection involves allocation of buffers for storing user data, synchronizing the sequence numbers of packets etc.
   - A connection is released at the request of upper layer.
2. Addressing
   - In order to deliver the message from one process to another, an addressing scheme is required. Several processes may be running on a system at a time.

   - In order to identify the correct process out of the various running processes, transport layer uses an addressing scheme called port number. Each process has a specific port number.
3. Data transfer
   - Transport layer breaks user data into smaller units and attaches a transport layer header to each unit forming a TPDU.
   - The TPDU is handed over to the network layer for its delivery to destination. The TPDU header contains port number, sequence number, acknowledgement number, checksum and other fields.
4. Flow control
   - Like data link layer, transport layer also performs flow control. However, flow control at transport layer is performed end-to-end rather than node-to-node.
   - Transport layer uses a sliding window protocol to perform flow control.
5. Error Control : Transport layer also provides end-to-end error control facility. It also deals with several different types of errors like damaged bits, non delivery and duplicate delivery of TPDUs.
6. Congestion Control : Transport layer also handles congestion in the networks. Several different congestion control algorithms are used to avoid congestion.

4.3 : Socket Programming

Q.5 What are the types of socket ? Explain various socket primitives used in connection oriented client server approach.

☞ [SPPU : Dec-17,19, May-18, End Sem, Marks 6]

OR What are three different types of sockets ? Explain various socket primitives used in connection oriented client server approach.

☞ [SPPU : May-19, End Sem, Marks 8]

Ans. : • Sockets allow communication between two different processes on the same or different machines. The socket is the combination of IP address and software port number used for communication between multiple processes.

- Types of socket are as follows :
  1. **Stream socket** : It uses TCP protocol. The stream socket (SOCK_STREAM) interface defines a reliable connection-oriented service. Data is sent without errors or duplication and is received in the same order as it is sent.
  2. **Datagram socket** : It uses UDP protocol. The datagram socket (SOCK_DGRAM) interface defines a connectionless service for datagrams or messages. Datagrams are sent as independent packets. The reliability is not guaranteed, data can be lost or duplicated and datagrams can arrive out of order.
  3. **Raw socket** : It uses IP and ICMP protocol. The raw socket (SOCK_RAW) interface allows direct access to lower-layer protocols such as Internet Protocol (IP).
- Socket primitive are as follows :
  - Before an application program can transfer any data, it must first create an end point for communication by calling socket. Socket facilities are provided in C language.
  - To use these facilities, the header files <types.h> and <socket.h> must be included in the program. Its prototype is

    int socket (int family, int type, int protocol) ;

    where the family identifies the family by address or protocol. The address family identifies a collection of protocol with the same address format, while the protocol family identifies a collection of protocols having the same architecture. The type identifies the semantics of communication.
  - After a socket is created, the bind system call can be used to assign an address to the socket. Its prototype is

    int bind (int sd, struct sockaddr *name, int namelen) ;

    where sd is the socket descriptor returned by the socket call, name is a pointer to an address structure that contains the local IP address and port number and nameless is the size of the address structure in bytes. The bind system call returns 0 on success and – 1 on failure.

  - A connection-oriented server indicates its response to receive connection request by calling listen the prototype is

    int listen (int sd, int backlog) ;

    where sd is socket descriptor returned by the socket call and backlog specifies the maximum number of connection requests that the system should queue while it waits for the server to accepts them.
  - Server can accept the connection request after listen call. The prototype for accept is :

    int accept (int sd, struct sockaddr *addr, int *addrlen) ;
  - After this client and server transmit data using write and read system calls. If the socket is not used for long time, socket is closed by using close system call. The prototype used for close call is :

    int close (int sd) ;

    If socket is closed successfully, it returns 0 otherwise – 1 for failure.

4.4 : Elements of Transport Layer Protocols

Q.6 Explain upward and downward multiplexing in transport layer.

Ans. : Multiplexing : • Many virtual circuits open for long periods of time is to make multiplexing of different transport connections onto the same network connection attractive. This form of multiplexing called **upward multiplexing.**

- Four distinct transport connections all use the same network connection to the remote host. The transport layer forms the group of transport connection according to their destination and map each group onto the minimum number of network connections.

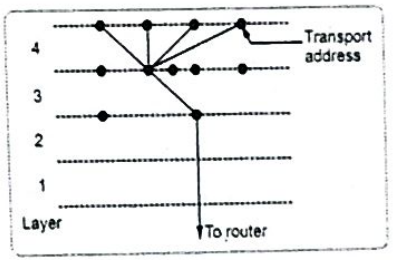


Fig. Q.6.1 (a) Upward multiplexing

- Many transport connections are mapped onto one network connection, the performance will be poor, because users will have to wait their turn

to send one message. If too few transport connections are mapped onto one network connection, the service will be expensive.

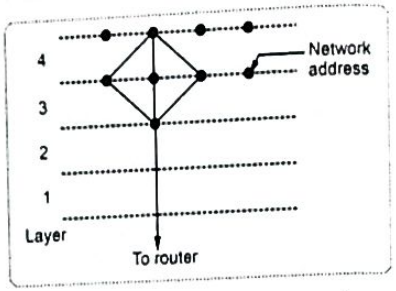


Fig. Q.6.1 (b) Downward multiplexing

- The transport layer opens multiple network connections and distributes the traffic among them on a round-robin basis. This is called **downward multiplexing.**
- With k network connections open, the effective bandwidth is increased by a factor of k. If multiple output lines are available, downward multiplexing can also be used to increase the performance even more.
- Fig. Q.6.1 shows the multiplexing.

Q.7 Explain transport layer crash recovery.

Ans. : Crash Recovery :

- If the host computer (server) and routers are subject to crashes, the recovery from these crashes makes some problem. If the network layer provides connection-oriented service, then the lost of data or virtual circuit is handled by establishing a new connection. Then retransmit the TPDUs, which has not received. If the host server crashes, then the client must quickly reboot.
- When the server crash while receiving data from client, the outstanding TPDU is lost. To recover the data, when the server comes back up, its tables are reinitialized, so it no longer knows precisely where it was.
- The server might send a broadcast TPDU to all other host, announcing that it had just crashed and requesting that its clients inform it for the status of all open connections. Client can be in one of two states : TPDU outstanding or no TPDU outstanding. Based on only this state information the client must decide whether or not to retransmit the most recent TPDU.

- To avoid the duplicate of data the client should retransmit only if it has an unacknowledged TPDU outstanding.
- There are many situation for crash recovery. If the server send acknowledge and crash the server before writing the data. The writing (saving data) data and sending acknowledgement, both are different process. So the server and client programmed in any way, the lost of data and duplicate of data may occurs.
- If both sides are programmed considering all situation, upto some limit it is possible to recover the lost data and possible to avoid retransmitting.

Q.8 Explain connection establishment and connection release with respect to the transport layer.

Ans. : i) Connection establishing : The connection establishment serves three main purposes.

1. It allows each end to assure that the other exists.
2. It allows negotiation of optional parameter like maximum segment size, maximum window size and quality of service.
3. It triggers allocation of transport entity resources like buffer space.

- There are three phases in any virtual connection. These are the connection establishment, data transfer and connection termination phases. In order for two hosts to communicate using TCP they must first establish a connection by exchanging messages in what is known as the three-way handshake.
- Fig. Q.8.1 shows the process of the three-way handshake.
- There are three TCP segments exchanged between two hosts, host A and host B. To start, host A initiates the connection by sending a TCP segment with the SYN control bit set and an Initial Sequence Number (ISN) here it is represent as the variable x in the sequence number field.
- At some moment later in time, host B receives this SYN segment, process it and responds with a TCP segment of its own. The response from host B contains the SYN control bit set and its own ISN represented as a variable y.
- Host B also sets the ACK control bit to indicate the next expected byte from host A should contain data starting with sequence number x+1.

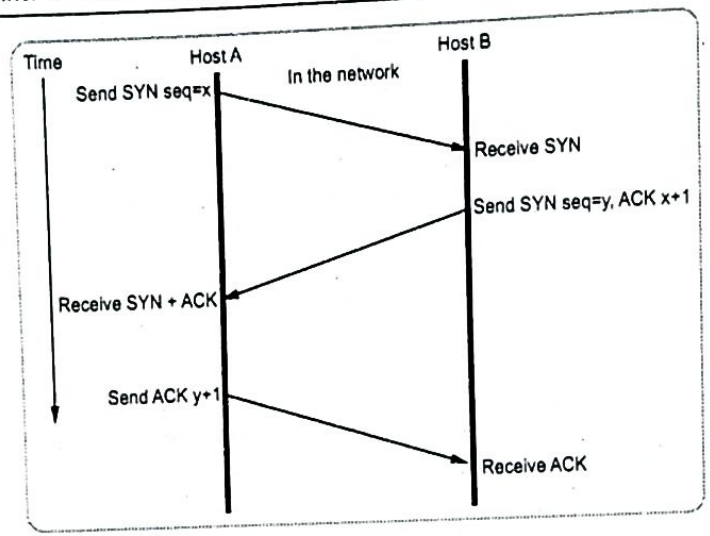


Fig. Q.8.1 TCP connection establishment

- When host A receives host B's ISN and ACK, it finishes the connection establishment phase by sending a final acknowledgement segment to host B. In this case, host A sets the ACK control bit and indicates the next expected byte from host B by placing acknowledgement number y+1 in the acknowledgement field.
- Once ISNs have been exchanged, communicating applications can transmit data between each other.

ii) **Connection Release :** In order for a connection to be released, four segments are required to completely close a connection. Four segments are necessary due to the fact that TCP is a full-duplex protocol, meaning that each end must shut down independently. The connection termination phase is shown in Fig. Q.8.2.

- Notice that instead of SYN control bit fields, the connection termination phase uses the FIN control bit fields to signal the close of a connection.
- To terminate the connection, the application running on host A signals TCP to close the connection. This generates the first FIN segment from host A to host B.
- When host B receives the initial FIN segment, it immediately acknowledges the segment and notifies its destination application of the

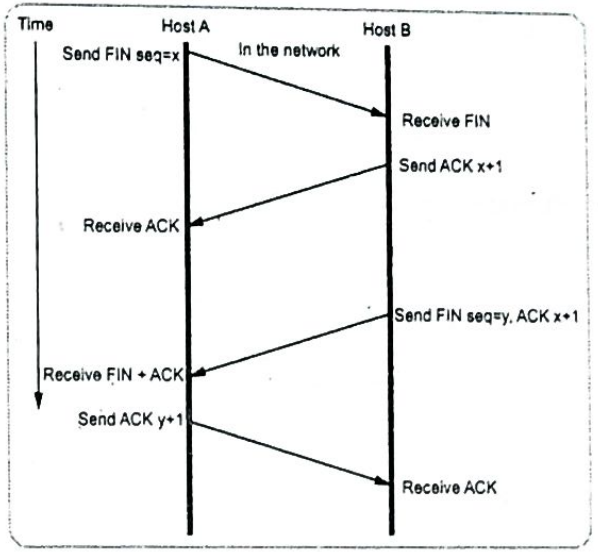


Fig. Q.8.2 Connection termination

termination request. Once the application on host B also decides to shut down the connection, it then sends its own FIN segment, which host A will process and respond with an acknowledgement.

Q.9 Write short note on flow control and buffering.

Ans. : • Flow control is implemented using modified form of sliding window protocol. The window size is variable and is controlled by the receiver. The receiver sends a credit allocation to the sender. The credit allocation indicates how many TDPU the receiver is ready to receive if the network service is unreliable, the sender must buffer all TDPUs sent. With reliable network service, if the sender knows that the receiver always has buffer space, it need not retain copies of the TPDU it sends.

- If the receiver cannot guarantee that every incoming TPDU will be accepted, the sender will have to buffer anyway. Even if the receiver has agreed to do the buffering, then the problem comes with buffer size.
- If most TPDUs are nearly the same size, it is natural to organize the buffers as a pool of identical size buffers, with one TPDU per buffer. If the buffer size is chosen equal to the largest possible TPDU, space will be wasted whenever a short TPDU arrives. If the buffer size is less than

the maximum TPDU size, multiple buffers will be needed for long TPDUs, with the attendent complexity.

4.5 : Congestion Control

Q.10 What is congestion and congestion control ?

Ans. : Congestion :

When too many packets rushing to a node or a part of network, the network performance degrades, and this situation is called as **congestion**. When the number of packets dumped into the subnet and as traffic increases the network is no longer able to cope and design losing packets at very high traffic, performance collapses completely and almost no packets are delivered.

Congestion control :

Congestion control is a process of maintaining the number of packets in a network below a certain level at which performance falls off. Congestion control makes sure that subnet is able to carry the offered traffic. So congestion control is different process than flow control.

Q.11 Explain Additive Increase, Multiplicative Decrease control (AIMD) TCP congestion control method.

Ans. : • TCP maintains a new state variable for each connection, called congestion window, which is used by the source to limit how much data it is allowed to have in transit at a given time. The congestion window represents the amount of data, in bytes.

- AIMD performs a slow increase in the congestion window size when the congestion in the network decreases and a fast drop in the window size when congestion increases.
- Let W_m be the maximum window size, in bytes, representing the maximum amount of unacknowledged data that a sender is allowed to send.
- Let W_a be the advertised window sent by the receiver, based on its buffer size.
- TCP's effective window is revised as follows :

  Max window = MIN (Congestion window, Advertised window)

Effective window = Max window – (Last byte sent – Last byte ACKed)

- **Max window** replaces **Advertised window** in the calculation of **Effective window.**
- Fig. Q.11.1 shows the additive increase control for TCP congestion control.

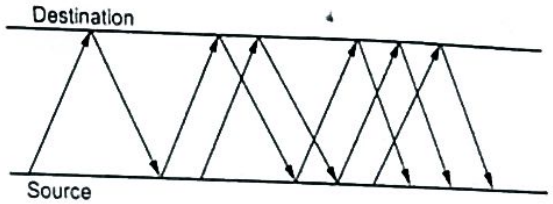


Fig. Q.11.1 AIDM

- The challenge in TCP congestion control is for the source node to find a right value for the congestion window. The congestion window size varies, based on the traffic conditions in the network. TCP watches for timeout as a sign of congestion.
- TCP technique requires that the timeout values be set properly. Two important factors in setting timeouts follow.
  1. Average round trip times (RTTs) and RTT standard deviation based to set timeouts.
  2. RTTs are sampled once every RTT is completed.

Q.12 Explain slow start method.

Ans. : • Slow start method increases the congestion window size nonlinearly and in most cases exponentially, as compared to the linear increase in additive increase.

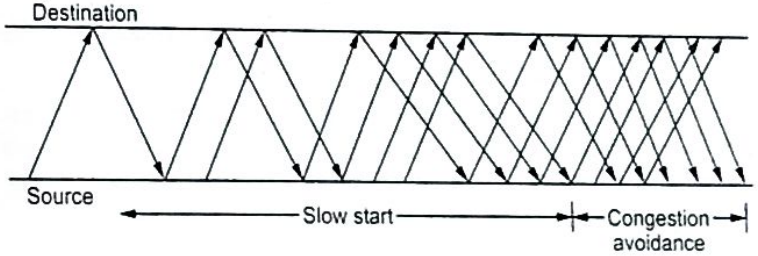


Fig. Q.12.1 Slow start

- Fig. Q.12.2 shows the slow start method. In this method, the congestion window is again interpreted in packets instead of bytes.
- Source initially sets the congestion window to one packet. When its corresponding acknowledgement arrives, the source sets the congestion window to two packets. Now, the source sends two packets. On receiving the two corresponding acknowledgements, TCP sets the congestion window size to 4. Thus, the number of packets in transit doubles for each round-trip time.
- The slow start method is normally used,
  1. Just after a TCP connection is set up.
  2. When a source is blocked, waiting for a timeout.

4.6 : Transport Layer Protocols : TCP

Q.13 Explain TCP header in detail.

[SPPU : May-18,19, End Sem, Marks 6]

Ans. : • Fig. Q.13.1 shows the format of the TCP header.

- Description of field in the TCP header as follows :
  1. **Source port :** It specifies the application sending the segment. This is different from the IP address, which specifies an internet address.
  2. **Destination port :** It identifies the receiving application port. numbers below 256 called well-known ports and are assigned to commonly used applications. For examples, port 23 corresponds to a Telnet function. Port 53 for DNS name server and port 21 assigned for FTP.
  3. **Sequence number :** Each byte in the stream that TCP sends is numbered. The sequence number wraps back to 0 after $2^{32} - 1$.
  4. **Acknowledgement number :** This field identifies the sequence number of the next data by the that the sender expects to receive if the ACK bit is set. If the ACK bit is not set, this field has no effect.

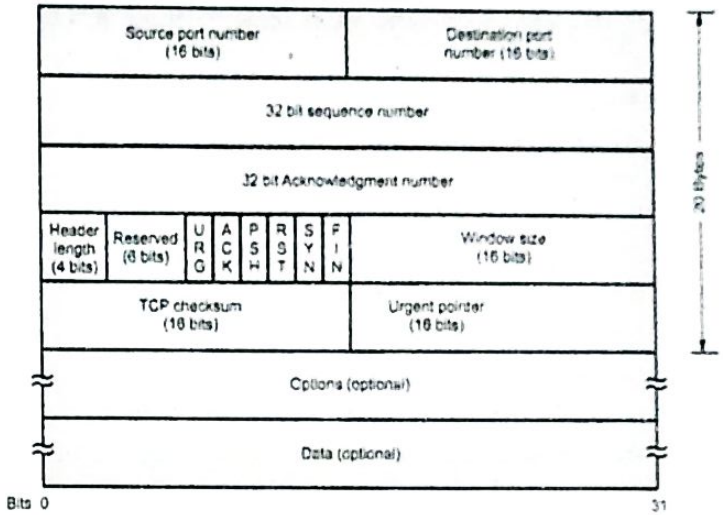


Fig. Q.13.1 TCP header format

5. **Header length :** It specifies the length of the TCP header in 32-bit words. Because of option field, header length is used.
6. **Reserved :** This field is reserved for future use and must be set to 0 (zero).
7. TCP header contains six flag bits. One or more than one can be turned on at the same time. The function of each flag is as follows.
   a. **URG :** The Urgent pointer is valid if it set to 1.
   b. **ACK :** ACK bit is set to 1 to indicate that the acknowledgement number is valid.
   c. **PSH :** The receiver should pass this data to the application as soon as possible.
   d. **RST :** This flag is used to reset the connection. It is also used to reject an invalid segment.
   e. **SYN :** Synchronize sequence number to initiate a connection. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.

- A typical value for MSS is 1460.
- TCP connections are full duplex. The steps required establishing and release connections can be represented in a finite state machine.

Q.15 Explain four steps of connection termination in TCP.

Ans. : • Any of the two parties involved in exchanging data can close the connection. When connection in one direction is terminated, the other party can continue sending data in the other direction.

- Four steps are required to close the connection in both direction. Fig. Q.15.1 shows four step connection termination.

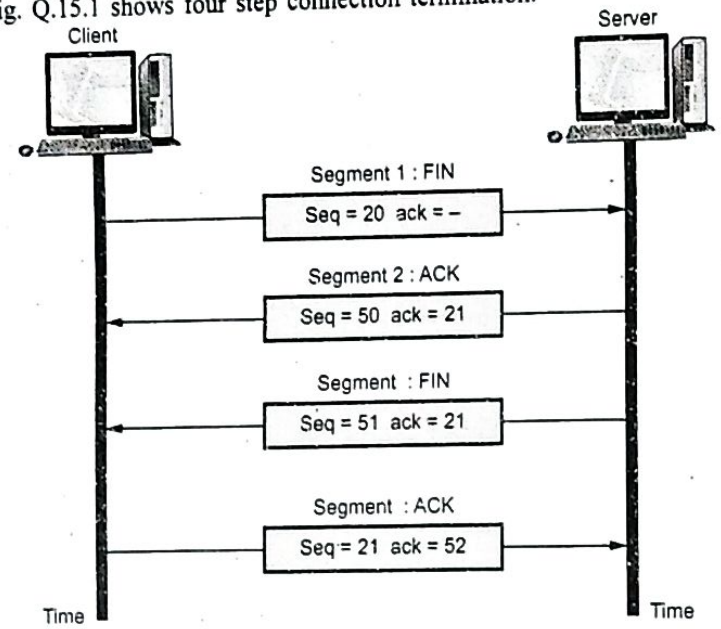


Fig. Q.15.1 Four steps connection termination

- **Steps are as follows :**
  1. The client TCP sends the first segment, a FIN segment.
  2. The server TCP sends the second segment, an ACK segment, to confirm the receipt of the FIN segment from the client.
  3. The server TCP can continue sending data in the server client direction. When it does not have any more data to send, it sends the third segment.

4. The client TCP sends the fourth segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server.

Q.16 What causes silly window syndrome ? How it is solved ? Explain with an example. ☞ [SPPU : April-17 (In Sem), Marks 5]

Ans. : Silly window syndrome :

- When large block of data is passed from sender but the receiver reads data one byte at a time. Receiving side, the TCP buffer is full and the sender know the condition. The interactive application reads one character from the TCP stream.
- Receiving TCP tells to the sender to send the only 1 byte. Sender send 1 byte. Now buffer is full and receiver send acknowledgement the 1-byte segment and set the window 0. This operation is continuous. Fig. Q.16.1 shows these steps.

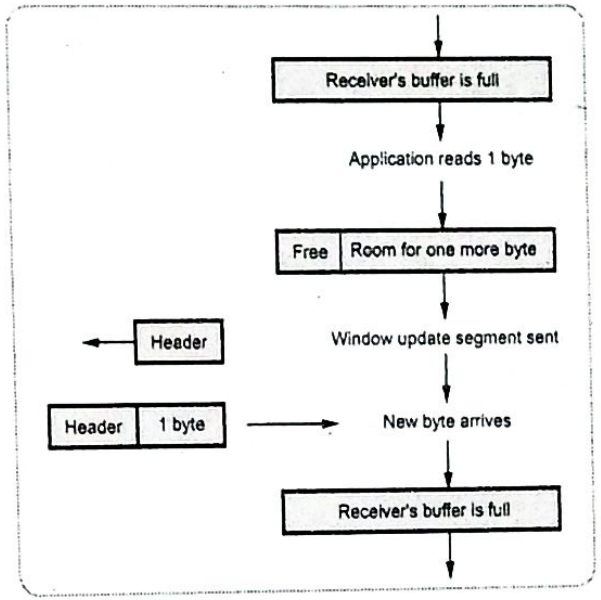


Fig. Q.16.1 Silly window syndrome

- Nagle algorithm and Clark's solution to the silly window syndrome are complementary. Clark solution is to prevent the receiver from sending a

window update for 1 byte. Instead it is forced to wait until it has a decent amount of space available.

Q.17 Differentiate between TCP and UDP.

☞ [SPPU : Dec.-18, 19, May-19, End Sem, Marks 6]

Ans. :

Sr. No.	TCP	UDP
1.	TCP is connection oriented.	UDP is connectionless.
2.	TCP connection is byte stream.	UDP connection is message stream.
3.	TCP does not support multicasting and broadcasting.	UDP support broadcasting.
4.	It provides error control and flow control.	It does not provide flow control and error control.
5.	TCP supports full duplex transmission.	UDP does not support full duplex transmission.
6.	TCP is reliable.	UDP is unreliable.
7.	TCP packet is called segment.	UDP packet is called user datagram.

Q.18 Explain TCP timers.

Ans. : • TCP manages four different timers for each connection.

a) A **retransmission timer** is used when excepting an acknowledgement from the other end.

b) A **persist timer** keeps window size information flowing even if the other end closes its receiver window.

c) A **keep alive timer** detects when the other end on an otherwise idle connection crashes.

d) A 2 **maximum segment lifetime** (2 MSL) timer measures the time a connection has been in the TIME_WAIT state.

Q.19 For each of the following applications, determine whether TCP or UDP is used as the transport layer protocol and explain the reasons(s) for your choice

i) Watching a real time streamed video.

ii) Web browsing.

iii) A Voice over IP (VoIP) telephone conversation.

iv) YouTube video.

☞ [SPPU : Dec.-17, End Sem, Marks 8]

Ans. : i) Watching a real time streamed video : This should be UDP. The reason is that when watching a movie, delay is critical and therefore there simply is not any time to seek the retransmission of any errors. The simplicity of UDP is therefore required.

ii) Web browsing : This should be TCP. The reason is that web pages need to be delivered without error so that all content is properly formatted and presented. Therefore the error detection and correction properties of TCP are needed.

iii) A Voice over IP (VoiP) telephone conversation : This should be UDP. The reason is that a telephone conversation has strict timing requirements for the transfer of data and seeking the retransmission of any errors would introduce too much delay. Therefore the simplicity of UDP is needed.

iv) YouTube video : This should be TCP. Video streaming adopts pre-fetching and buffering to achieve smooth play-out. TCP provides such (network} buffer, as well as the reliable transmission guarantee for no loss of frame.

Q.20 Explain state transition diagram of TCP.

☞ [SPPU : Dec-18, 19, End Sem, Marks 6]

Ans. : TCP Finite State Machine :

- Fig. Q.20.1 shows finite state machine.
- The lightface lines are unusual event sequences. Each line in Fig. Q.20.1 is marked by an event/action pair. The event can either be a user-initiated system call (CONNECT LISTEN, SEND or CLOSE), a segment arrival (SYN, FIN, ACK or RST) or in one case, a timeout of twice the maximum packet lifetime. The action is the sending of a control segment (SYN, FIN, or RST) or nothing, indicated by ---. Comments are shown in parentheses.

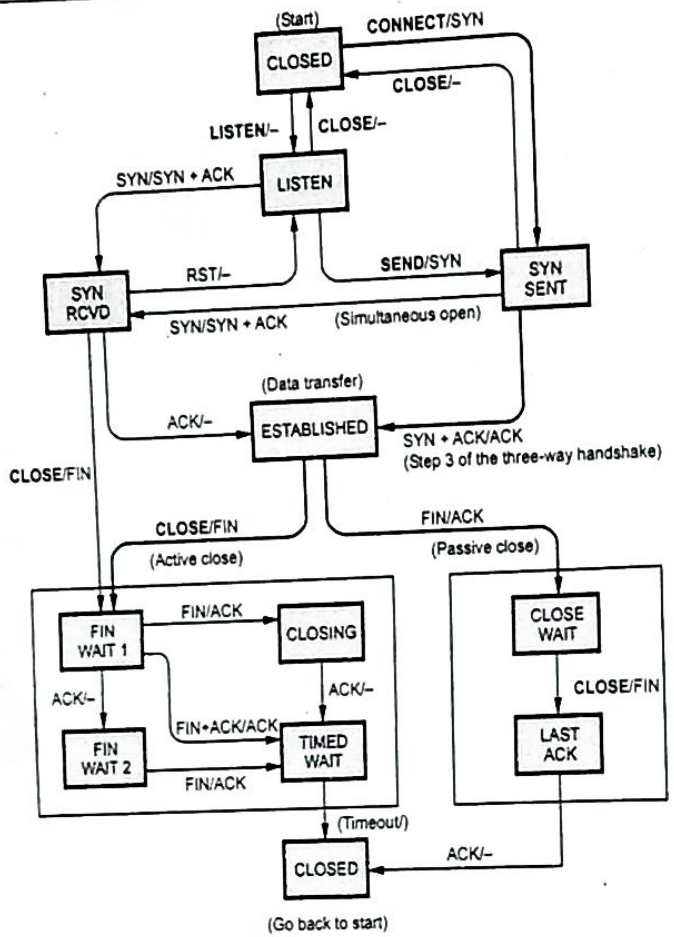


Fig. Q.20.1 TCP finite state machine

- The states used in the TCP connection management finite state machine are as follows :

State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call

SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

- The diagram can best be understood by first following the path of a client (the heavy solid line) then later the path of a server (the heavy dashed line). When an application on the client machine issues a CONNECT request, the local TCP entity creates a connection record, marks it as being in the SYN SENT state, and sends a SYN segment.
- Note that many connections may be open (or being opened) at the same time on behalf of multiple applications, so the state is per connection and recorded in the connection record. When the SYN + ACK arrives. TCP sends the final ACK of the three-way handshake and switches into the ESTABLISHED state data can now be sent and received.
- When an application is finished, it executes a CLOSE primitive, which causes the local TCP entity to send a FIN segment and wait for the corresponding ACK (dashed box marked active close).
- When the ACK arrives, a transition is made to state FIN WAIT 2 and one direction of the connection is now closed. When the other side closes, too, a FIN comes in, which is acknowledged. Now both sides

are closed, but TCP waits a time equal to the maximum packet lifetime to guarantee that all packets from the connection have died off, just in case the acknowledgement was lost. When the timer goes off, TCP deletes the connection record.

- Connection management from server view point, sever does a LISTEN and settles down to see who turns up. When a SYN comes in, it is acknowledged and the server goes to the SYN ACK state. When the server's SYN is itself acknowledged, the three way handshake is complete and the server goes to the ESTABLISHED state. Data transfer can now occur.

4.7 : Transport Layer Protocols : UDP, SCTP, RTP

Q.21 Explain UDP protocol header format.

Ans. : • Fig. Q.21.1 shows the format of the UDP header. The port number identify the sending process and the receiving process.

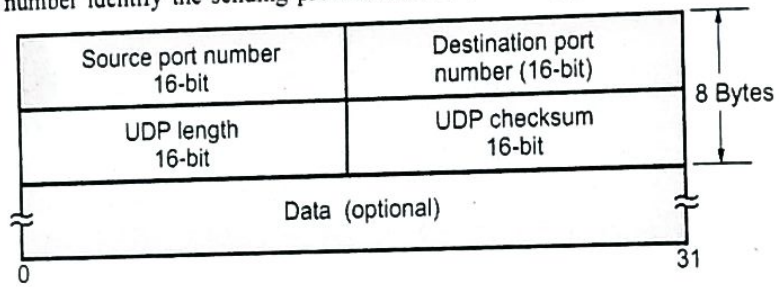


Fig. Q.21.1 UDP header

- The UDP datagram contains a source port number and destination port number. Source port number identifies the port of the sending application process. The destination port number identifies the receiving process on the destination host machine.
- The UDP length field is the length of the UDP header and the UDP data in bytes. The minimum value for this field is 8 bytes.
- UDP checksum covers the UDP header and the UDP data. Both UDP and TCP include a 12 byte pseudo-header with the UDP datagram just for the checksum computation. This pseudo_header includes certain

fields from the IP header. The purpose is to let UDP double check that the data has arrived at the correct destination.

- UDP checksum is end-to-end checksum. It is calculated by the sender, and then verified by receiver. It is designed to catch any modification of the UDP header or data anywhere between sender and receiver.

Q.22 Explain RTP protocol in detail.

[SPPU : May-19, Dec-19, End Sem, Marks 8]

Ans. : • Fig. Q.22.1 shows the RTP header. RTP header size is 32 bits. Fields in the headers are version, P, X, CC, M, payload type, sequence number, timestamp, synchronization source identifier and contributing source identifier.

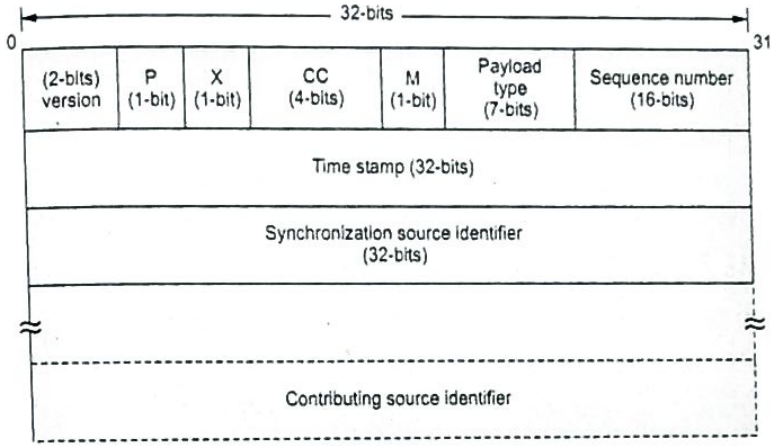


Fig. Q.22.1 RTP header

1. **Version :** Size of version field is 2-bits. It indicates version number. The current version is 2.
2. **P bit :** Size is 1-bit. P bit indicates that the packet has been **padded** to a multiple of 4 bytes.
3. **X-bit :** Size is again 1-bit and it indicates that the **extension** header is present.
4. **CC field :** Size of CC field is 4-bits. CC field is used for indicating number of source present. The range is from 0 to 15.

5. **m bit :** Marker bit is of 1-bit size. This bit is used to indicate start of the frame. It may be video frame, start of a word in an audio channel.
6. **Payload type :** Size of the payload type field is 7-bits. This field is used for indicating encoding algorithm has been used. It determines its interpretation by the application.
7. **Sequence number :** This 16-bit field is incremented by one each time an RTP packet is sent. The number can be used by the receiver to detect packet loss and to recover packet sequence. The initial value is selected at random.
8. **Time stamp :** It is 32-bits number specifies the sampling instant of the first byte in the RTP data packet. This value can help to reduce jitter at the receiver by decoupling the playback from the packet arrival time. The initial value is selected at random.
9. **Synchronization source identifier :** This field tells which stream the packet belongs to. It is the method used to multiplex and demultiplex multiple data streams onto a single stream of UDP packets.
10. **Contributing source identifier :** This list of 0 to 15 thirty-two bit items specifies the contributing sources for the payload contained in the packet. This field is used when mixers are present in the studio.

Q.23 Explain UDP header ? Below is an hexadecimal dump of an UDP datagram captured.

e2 a7 00 0D 00 20 74 9e 0e ff 00 00 00 01 00 00 00 00 00 00 06 69 73 61 74 61 70 00 00 01 00 01

i) What is source port number ?

ii) What is destination port number ?

iii) What is total length of the user datagram ?

iv) What is the length of the data ?

v) Is packet directed from a client to server or vice versa ?

[SPPU : Dec.-17, End Sem, Marks 8]

Ans. : UDP header : Refer Q.21.

i) The source port number is the first four hexadecimal digits {e2a7), which means thc1t the source port number is 58023.

ii) The destination port number is the second four hexadecimal digits (OOOD), which means that the destination port number is 13.

iii) The third four hexadecimal digits (0020) define the length of the whole UDP packet as 32 bytes.

iv) The length of the data is the length of the whole packet minus the length of the header, or 32-8 = 24 bytes.

v) Since the destination port number ls 13 {well known port), the packet is from the client to the server.

Q.24 Below is an hexadecimal dump of an UDP datagram captured.

06 32 00 0D 00 1C E2 17

i) What is source port number ?

ii) What is destination port number ?

iii) What is the length of the data ?

iv) Is packet directed from a client to server or vice versa ?

[SPPU : May-18, Dec-18, End Sem, Marks 4]

Ans. : i) Source port number = $(0632)^{16}$ = 1586

ii) Destination port number = $(000D)^{16}$ = 13

iii) Total length = $(001C)^{16}$= 28 bytes

iv) Since the header is 8 bytes the data length is 28 – 8 = 20 bytes.

v) From a client to a server

vi) Daytime

Q.25 Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How may total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment ?

[SPPU : Dec.-18, End Sem, Marks 6]

Ans. :

User data = 8880 bytes

MTU = 1500 bytes

8880 headers = 8 bytes

IP headers = 20 bytes

Header length = 20 + 8 = 28 bytes

Actual data in each fragments = 1500 – 28 = 1472 bytes

Fragments	Data	Headers	Offsets
1st	1472	28	0/8 = 0
2nd	1472	28	1472/8 = 184
3rd	1472	28	1472 × 2 / 8 = 368
4th	1472	28	1472 × 3 /8 = 552
5th	1472	28	1472 × 4 / 8 = 736
6th	1472	28	1472 × 5 / 8 = 920
7th	48	28	1472 × 6 / 8 = 1104

Number of IP fragments will be 7

Offset field of last fragments is 1104

So the correct options is "C"

Q.26 Write short note on SCTP.

Ans. : • SCTP is a reliable transport protocol operating on top of a potentially unreliable connectionless packet service such as IP. It offers acknowledged error-free non-duplicated transfer of datagrams (messages). Detection of data corruption, loss of data and duplication of data is

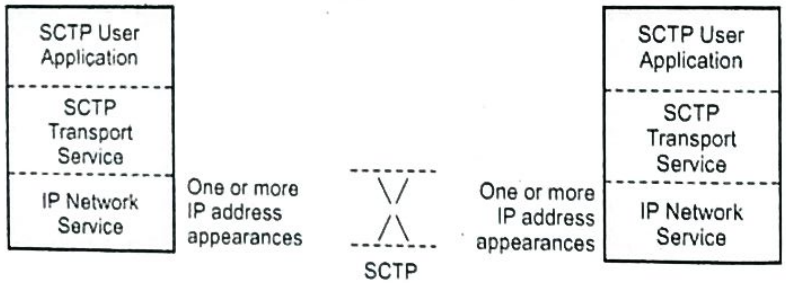


Fig. Q.26.1 Diagram showing the concept of SCTP association

achieved by using checksums and sequence numbers. A selective retransmission mechanism is applied to correct loss or corruption of data.

- **Stream Control Transmission Protocol** (SCTP) is a Ttransport Layer Protocol, serving in a similar role as the popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with congestion control.
- An SCTP association generally looks like this, so the services of SCTP are naturally at the same layer as TCP or UDP services :

Q.27 Explain SCTP services.

Ans. : • Similar to TCP, SCTP provides a reliable and in-order data transfer service to HTTP. Additionally, SCTP provides other services unavailable in TCP. These services are summarized below.

1. Multistreaming.
2. Process to process communication.
3. Four-way handshake during association establishment.
4. No Maximum Segment Lifetime (MSL) during association termination.
5. Multihoming for improved fault tolerance.
6. Preserving application message boundaries.
7. Reliable services.
8. Connection oriented service.
9. Sequenced delivery of user datagrams within a stream.

4.8 : Congestion Control and Quality of Service (QoS), Differentiated Services

Q.28 Write short note on RSVP.

Ans. : • RSVP is a signalling protocol used to reserve resources in the Internet. RSVP is a bandwidth reservation protocol.

- RSVP protocol allows applications to reserve bandwidth for their data flows.

Characteristics of RSVP

1. It provides reservations for bandwidth in multicast trees.
2. RSVP is receiver-oriented i.e. receiver intitiates this protocol for resource reservation.

- To get better reception and eliminate congestion any of the receivers in a group can send a reservation message up the tree to the sender. The message is propagated using the reverse path forwarding algorithm. Example of such a reservation is shown in the Fig. Q.28.1.

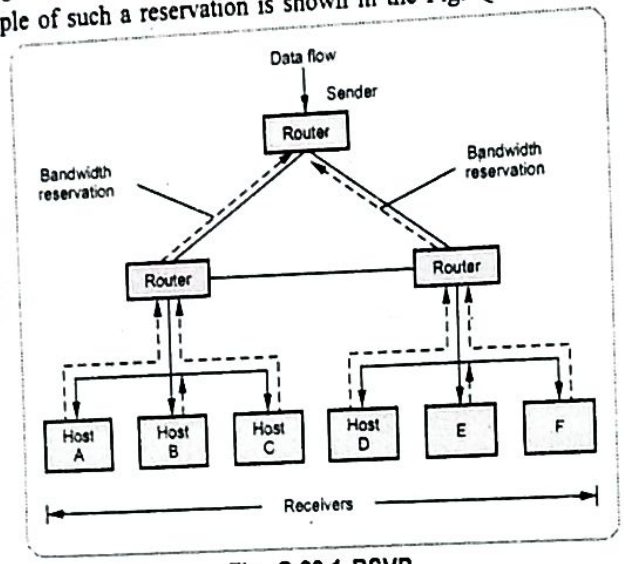


Fig. Q.28.1 RSVP

- Fig. Q.28.1 shows multicast spanning tree with data flowing from the top of the tree to hosts at the bottom of tree. The data originates from the sender and reservation message is originates from the receiver. The upstream reservation messages from host can be merged with other reservation message.

Q.29 List and explain fundamental elements of differentiated services.

Ans. : • The Differentiated Services (DiffServes) architecture consists of two sets of functioal elements :

1. Edge functions 2. Core functions

1. Edge functions :

- The packets arriving at the edge of network are marked. The mark of the packet defines the class of traffic to which it belongs. Depending on the mark, the packet may be immediately forwarded into the network, delayed or discarded.
- Edge functions are also called packet classification and traffic conditioning.

2. Core functions :

- On forwarding the packet by router it is then put on for next hop according to per hop behavior. The per hop behavior influences how router's buffer and BW are shared. It is a forwarding function of differentiated services (diffserv).
- Fig. Q.29.1 shows a logical view of classificaton and marking function within the edge7 router.

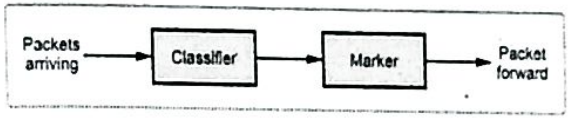


Fig. Q.29.1 Packet classification and marking

Q.30 What is policing ? Explain criteria for policing.

Ans. : Policing is the regulation of the rate at which packet flow is injected into the network.

Criteria for policing

- Three important policing criteria are identified, these are :

1. Average rate 2. Peak rate 3. Burst size

1. Average rate : Average rate is defined as packets per time interval. The average rate of packets in a network can be limited as a policy. This limits the traffic in the network for a long period of time.

2. Peak rate : Peak rate is defined as maximum number of packets that can be sent over a short period of time over a network.

3. Burst size : Burst size is the maximum number of packets that can be sent into the network over a extremely short interval of time.

Q.31 What are the techniques to improve Quality of Service (QoS) ?

[SPPU : Dec.-19, End Sem, Marks 6]

Ans. : • There are four techniques to improve quality of service : Scheduling, traffic shaping, resource reservation and admission control.

- An admission control, which is a quality of service mechanism, can also prevent congestion in virutal circuit networks. Admission control in ATM operates at the connection level and is therefore called connection admission control.
- Switches in a flow first check the resource requirement of a flow before admitting it to the network.
- A router can deny establishing a virtual circuit connection if there is congestion in the network.
- A source initiating a new flow must first obtain permission from an admission control entity that decides whether the flow should be accepted or rejected.
- The QoS may be expressed interms of maximum delay, loss probability, delay variance, or other performance parameters. If the quality of service of the new flow can be satisfied without violating QoS of existing flows, the flow is accepted; otherwise, the flow is rejected.

Q.32 Explain token bucket and leaky bucket algorithm with diagram.

[SPPU : Dec.-15, Marks 8]

Ans. : Traffic shaping is an open loop method of congestion control. Two types of algorithm are used for traffic shaping.

1. Leaky bucket algorithm 2. Token bucket algorithm

Leaky Bucket Algorithm

- Leaky bucket i.e. a bucket with a small hole in the bottom is used to store the water. The outflow from hole is at constant rate and irrespective of rate of entering water. Once the bucket is full, any additional water entering it spills over the sides and is lost.
- The same idea can be applied to packets. This is similar to a single server queueing system with constant service time.

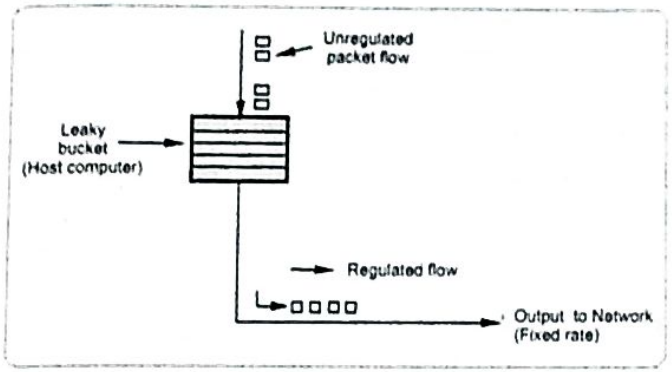


Fig. Q.32.1 Leaky bucket regulator

- Each host is connected to network with a finite internal queue. The host is allowed to put one packet per second on to the network. If a packet

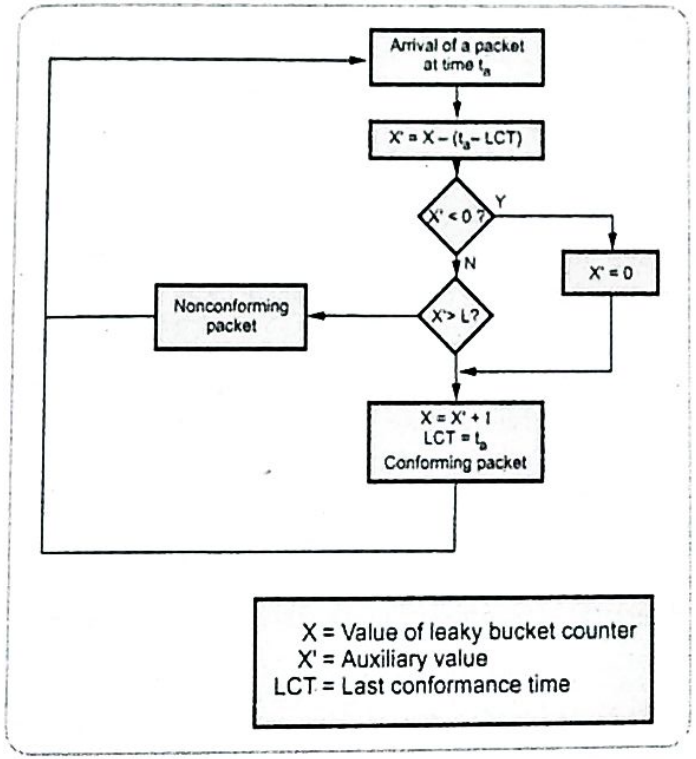


Fig. Q.32.2 Leaky bucket algorithm

arrives at the queue when it is full, the packet is discarded. This mechanism turn an unregulated traffic of the host regulated traffic on the network. Thus bursty traffic is smoothening and chances of congestion are reduced. Fig. Q.32.2 illustrates this algorithm.

- A leaky bucket regulator allows controlling the average rate, largest burst from a source. A leaky bucket regulator has both a packet bucket and a data buffer. Packets that arrive to the regulator that cannot be sent immediately are delayed in the data buffer.

Leaky Bucket Algorithm

- Fig Q.32.2 shows leaky bucket algorithm.

  X = Value of leaky bucket counter

  X' = Auxiliary value

  LCT = Last conformance time

- At the arrival of the first packet, the content of the bucket X is set to zero and the last conforming time is set to the arrival time of the first packet. The depth of the bucket is L+I where L typically depends on the traffic burstiness.

Token Bucket Algorithm

- The leaky bucket holds tokens. These tokens are generated by a clock at the rate of one token for every T sec. In token bucket bursts of up to n packets can be sent at once, which gives faster response to sudden bursts of input.
- The regulator collects tokens in a bucket, which fills-up at steady drip rate by packets. When a packet arrives at the regulator, the regulator sends the packet if the bucket has enough tokens. Otherwise, the packet waits either until the buckets has enough tokens. If the bucket is already fill of tokens, incoming tokens overflow and are not available to future packets. Thus, at any time, the largest burst a source can send into the network is roughly proportional to the size of the leaky bucket.
- Fig. Q.32.3 shows token bucket regulator.
- The regulator delays a packet if does not have sufficient number of tokens for transmission. A counter keeps track of tokens, the counter is

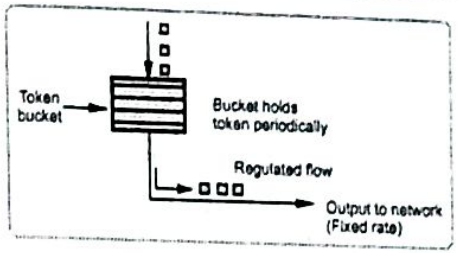


Fig. Q.32.3 Token bucket regulator

incremented by one every T and decremented by one whenever a packet is sent. When the counter hits zero, no packets may be sent. Smoother traffic can be obtained by putting a leaky bucket after the token bucket.

Q.33 Compare leaky bucket and token bucket.

Ans. : Comparison between leaky bucket and token bucket

Sr. No.	Leaky Bucket (LB)	Token Bucket (TB)
1.	Leaky bucket discards packets.	Token bucket discards tokens.
2.	With LB, a packet can be transmitted if the bucket is not full.	With TB, a packet can only be transmitted if there are enough tokens to cover its length in bytes.
3.	LB sends the packets at an average rate.	TB allows for large bursts to be sent faster by speeding up the output.
4.	LB does not allow saving, a constant rate is maintained.	TB allows saving up tokens (permissions) to send large bursts.

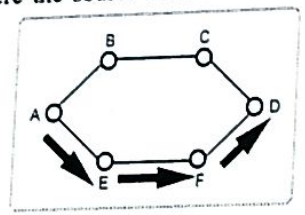
Q.34 Write short note on choke packet.

Ans. : • Another mechanism for congestion control is by using choke packets. This choke packet will have the effect of stopping or slowing down the rate of transmission from sources and hence limit the total number of packets in the networks. This approach requires additional

traffic on the network during a period of congestion. This can be applicable to both virtual circuit and datagram subnets.

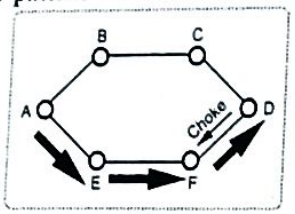
- When line utilization increases above some specific value called threshold, the line enters a 'alarming' situation. Each newly arriving packet is checked to see if its output line is in alarming state. If so, the router sends the said choke packet back to the source. This choke packet contains the destination address, so the source will not generate any more packets along the path.
- The traffic is reduced by adjusting parameters window size or leaky bucket output rate. Typically, the first choke packet causes the data rate to 50 % of its previous value the choke packet reduces the traffic to 25 % and so on.
- Congestion control using choke packets can be done by two ways. In first type the choke packet affects only source and in the second type the choke packet affects each hop it passes through. Fig. Q.34.1 shows choke packet that affects only the source.
- Fig. Q.34.1 shows a choke packet that affects each hop it passes through.

i) A subnet with six nodes A, B, C, D, E and F is shown in Fig. Q.34.1 (a). Here the source node is A and destination node is D.



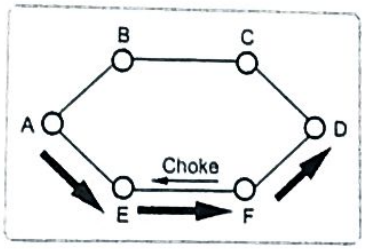
(a)

ii) When link utilization increased above its threshold, destination node D starts sending choke packets towards source node A.



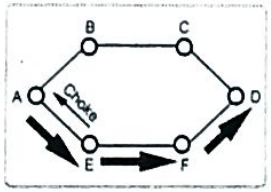
(b)

iii) The choke packets travels through the shortest or same path as that of packets.



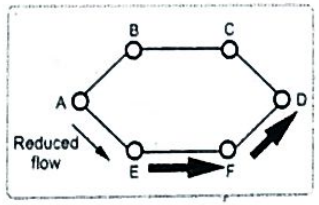
(c)

iv) The choke packet reaches to the source node A.



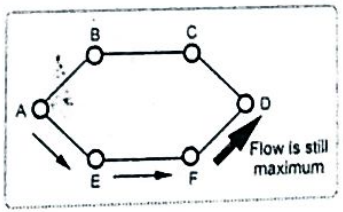
(d)

v) After receiving first chock packet source node A reduces its flow towards destination.



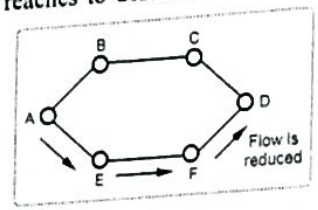
(e)

vi) The reduced packet flow follows the same reversed path i.e. the path of choke packets through various nodes.



(f)

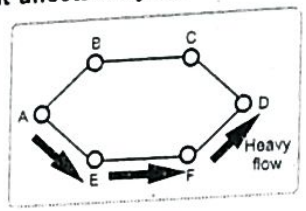
vii)The reduced flow reaches to destination node D.



(g)

Fig. Q.34.1 A choke packet that affects only the source

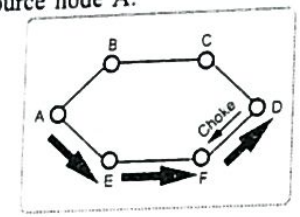
Fig. Q.34.2 shows a choke packet that affects each hop it passes through.



(a)

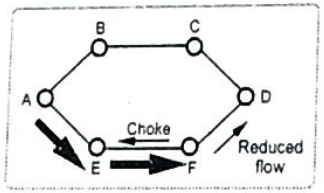
i) For the same subnet having nodes A, B, C, D, E and F source node and destination node D.

ii) When link utilization increased above its threshold destination node D starts sending choke packets towards source node A.



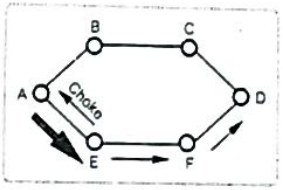
(b)

iii) The chock packets follows the exactly reversed path of traffic flowing packets. Here the chock packet reaches to node F. Immediately after reaching choke packet at node F, the traffic flow towards node D reduces.



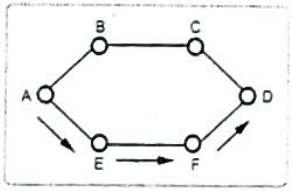
(c)

iv) As choke packet crosses node E, the traffic flow between nodes E, F, and F, D is reduced.



(d)

v) After reaching choke packet to source node A, the traffic flow between node A and node E and hence up to the destination node D is reduced.



(e)

Fig. Q.34.2 A choke packet that affects each hop it passes

Hop-by-hop choke packets

- Over long distances or at high speeds, the choke packets are not very effective.
- A more efficient way is to send choke packets hop-by-hop.
- A congested node would again generate a choke pocket, but each hop would be needed to reduce its transmission even before the choke packet arrives at the source.

4.9 : TCP and UDP for Wireless Networks

Q.35 Write short note on TCP and UDP for wireless networks.

Ans. : • TCP should not care whether IP is running over which media i.e. fiber or radio. Wireless transmission links are highly unreliable. They lose the packets all the time. The proper approach to dealing with lost packets is to send them again and as quickly as possible. When a packet

is lost on a wired network, the sender should slow down. When one is lost on a wireless network, the sender should try harder. When the sender does not know what the network is, it is difficult to make the correct decision.

- Frequently, the path from sender to receiver is inhomogeneous. It uses both, wired network and wireless network. The wireless TCP is split into two separate connection, as shown in the Fig. Q.35.1.

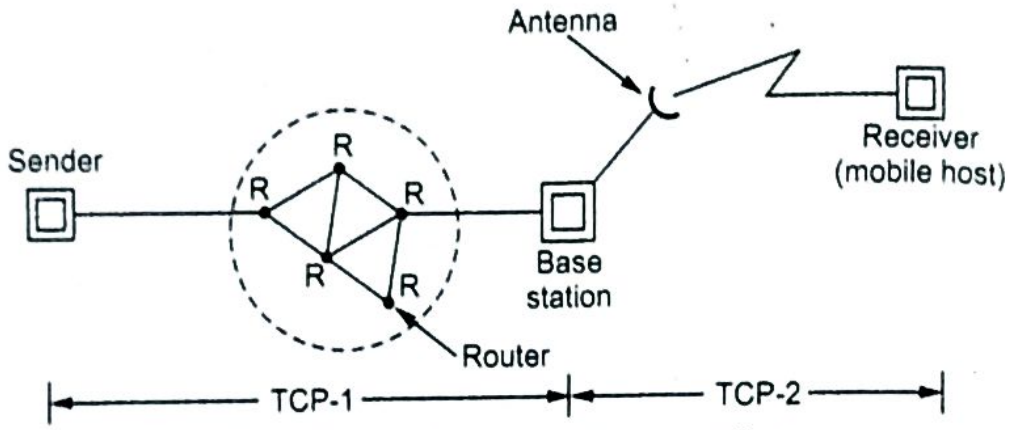


Fig. Q.35.1 Wireless TCP connection

- In TCP-1, connection goes from the sender to the base station. i.e. first stage. Mobile host (Receiver) gets data from base station antenna in TCP-2. The base station simply copies packets between the connections in both directions. This scheme solve the time out problem. Both connection, sender to base station and base station to receiver are homogeneous.
- Timeouts on the first connection can slow the sender down, whereas timeout on the second one can speed it up. Other parameter can also be tuned separately for two connections.
- The disadvantage of this scheme is, to break the TCP into two segments. UDP does not suffer from the same problem as TCP, wireless communication also introduces difficulties for it. The main trouble is that programs use UDP expecting it to be highly reliable. Wireless communication also affects areas other than just performance.

END...

Unit V

5 Application Layer

5.1 : Web

Q.1 What is web ? Explain content of web.

Ans. : • World wide web is collection of millions of files stored on thousands of servers all over the world. These files represent documents, pictures, video, sounds, programs, interactive environments.

• Following are hardware, software and protocols that make up the web.

1. A web server is a computer connected to the Internet that runs a program that takes responsibility for storing, retrieving and distributing some of the web files. A web client (web browser) is a computer that requests files from the web.
2. Well-defined set of languages and protocols that are independent of the hardware or operating system are required to run on the computers.
3. The Hyper Text Markup Language (HTML) is the universal language of the web.
4. Java is a language for sending small applications over the web. Java script is a language for extending HTML to embed small programs called scripts in web pages. The main purpose of Java and scripts is to speed up the interactivity of web pages.
5. VB script and Activex controls are microsoft system that work with IE.
6. Pictures, drawings, charts and diagrams are displayed on web using image formats such as JPEG and GIF formats.
7. The Virtual Reality Modeling Language (VRML) is the web's way of describing three-dimensional objects.

- A web page is an HTML document that is stored on a web server. A web site is a collection of web pages belonging to a particular organization.
- URL of these pages share a common prefix, which is the address of the home page of the size. Search engines are a bottom-up approach for finding your way around the web. Some search engines search only the titles of web pages. While other search every word. Keywords can be combined with Boolean operations, such as AND, OR and NOT, to produce rather complicated queries.
- Home page is the front door of a web site. When a person or organization says "My web site is at www.sangeeta.com", the URL to which they refer is the URL of the site's home page. The home page introduces the rest of the web site and provides links that leads to other pages on the site.

Q.2 Explain working of client-side and server-side of WWW.

Ans. : 1. The client side

- When a user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to.
  1. The browser determines the URL.
  2. The browser asks DNS for the IP address of www.vtubooks.com.
  3. DNS replies with 172.16.16.1.
  4. The browser makes a TCP connection to port 80 on 172.16.16.1.
  5. It then sends over a request asking for file/home/index.html.
  6. The www.vtubooks.com server sends the file/home/index.html.
  7. TCP connection is released.
  8. The browser displays all the text in home/index.html.
  9. The browser fetches and displays all images in this file.
- Fig. Q.2.1 shows the web model.

2. The server side

- The steps that the server performs.
  1. Accept a TCP connection from a client browser.

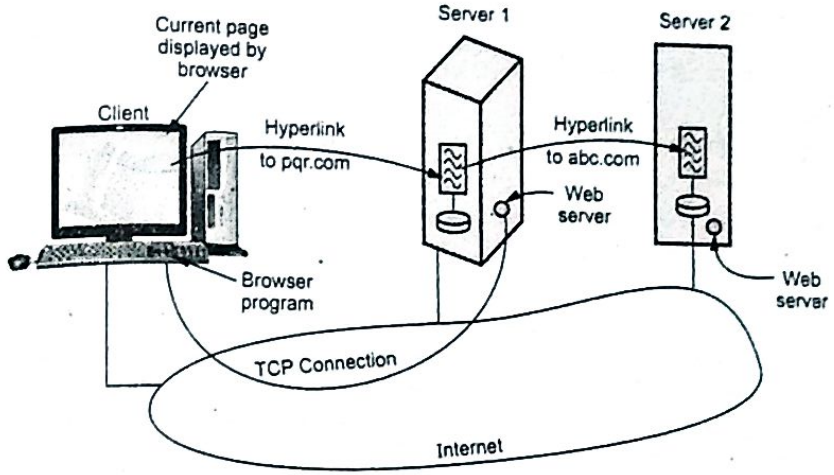


Fig. Q.2.1 Web model

  2. Get the name of the file required.
  3. Get the file.
  4. Return the file to the client.
  5. Release the TCP connection.

Q.3 What is statelessness and cookies ? Explain field used in cookies.

Ans. : • The web is basically stateless. There is no concept of a login session. The browser sends a request to a server and gets back a file. Then the server forgets that it has ever seen that particular client.

- When a client requests a web page, the server can supply additional information along with the requested page. This information may include a cookie, which is a small file. Browsers store offered cookies in a cookies directory on the client's hard disk unless the user has disabled cookies.
- Cookies are just files or strings, not executable programs. In principle, a cookie could contain a virus, but since cookies are treated as data there is no official way for the virus to actually run and do damage.
- A cookie may contain upto five fields.

  a) Domain b) Path c) Content

  d) Expires e) Secure

a) **Domain** : It tells where the cookies came from. Browsers are supposed to check that servers are not lying about their domain. Each domain may store no more than 20 cookies per client.

b) **Path** : The path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie. It is often 1, which means the whole tree.

c) **Content** : It takes the form name = Value. Both name and value can be anything the server wants. This field is where the cookies content is stored.

d) **Expires** : The expires field specifies when the cookies expires. If this field is absent, the browser discards the cookies when it exits. Such a cookies is called a **non-persistent cookie.** If a time and date are supplied, the cookie is said to be **persistent** and is kept until it expires.

e) **Secure** : This field can be set to indicate that the browser may only return the cookie to a secure server. This feature is used for e-commerce, banking and other secure applications.

Q.4 Explain common gateway interface.

Ans. : • CGI makes dynamic computation of web pages possible. It allows a web server to associate some URLs with computer program instead of static documents on disk.

- When a browser request one of the special URLs the server runs the associated computer program and sends the output from the program back to the user. A server can have an arbitrary number of CGI programs that perform different computations.
- The server uses the URL in the incoming request to determine which CGI program to run. CGI working is as follows : CGI program is part of a web server.
- The browser sends a request to the server. If the requested URL corresponds to a CGI program, the server starts the appropriate program and passes to the program a copy of the request.
- The server then sends the output from the CGI program back to the browser in the form of reply.

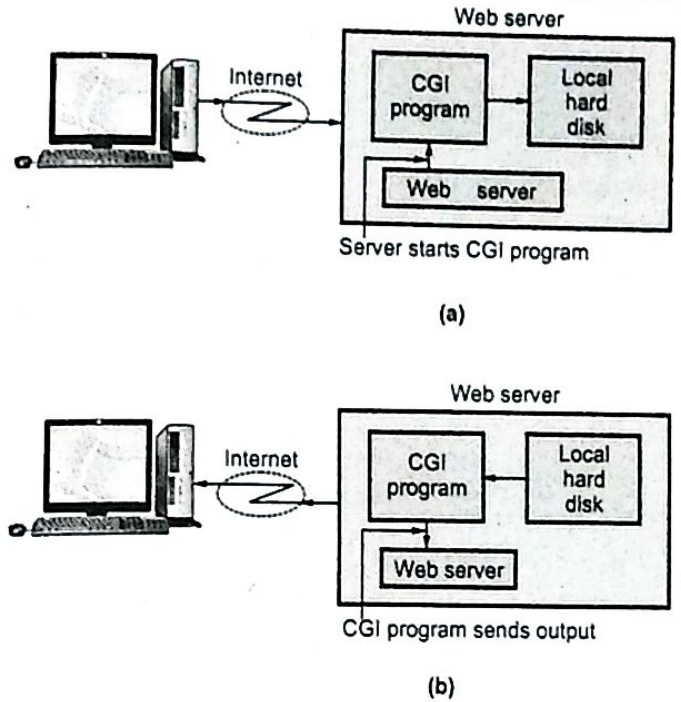


Fig. Q.4.1 Illustrates the CGI concepts

- From a browser's point of view, there is no difference between a URL that corresponds to a static document and one that corresponds to a CGI program. Requests for both static documents and CGI output have the same syntatic form.

5.2 : HTTP

Q.5 Explain HTTP request and reply message format.

[SPPU : May-18, Dec.-18,19, End Sem, Marks 6]

Ans. : • HTTP messages are two types

1. Request 2. Response

- Both message type used same format.
- Request **message** consists of a request line, headers and a body. Fig. Q.5.1 shows request message.

Request line

- Request line defines the

1. Request type
2. Resource
3. HTTP version

- Request type categorizes the request message into several methods for HTTP version 1.1.
- Fig. Q.5.2 shows the request line.
- URL is a standard for specifying any kind of information on the internet.
- The URL define four things,

1. Method 2. Host computer 3. Port 4. Path

- Fig. Q.5.3 shows the URL.

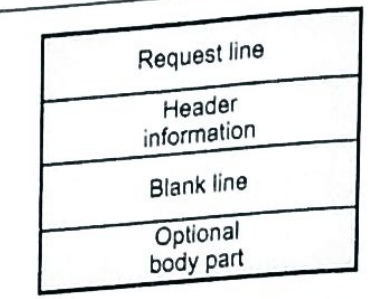


Fig. Q.5.1 Request message

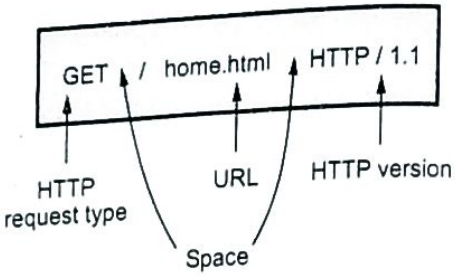


Fig. Q.5.2 Request line

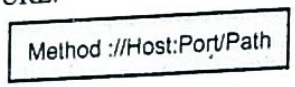


Fig. Q.5.3 (a) URL

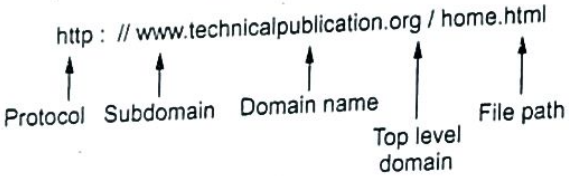


Fig. Q.5.3 (b) URL example

- The method is the prototocol used to retrieve the document. Several different protocols can retrieve a document, among them are FTP and HTTP.
- The host is the computer where the information is located, although the name of the computer can be alias. Web pages are usually stored in

computers and computers are given alias names that usually begin with the character www.

- The URL can optionally contain the port number of the server.
- Path is the path name of the file where the information is located.
- The request type field in a request message defines several kinds of messages referred to as methods.

Q.6 What is difference between persistent and non-persistent HTTP ? Explain HTTP request and reply message format.

[SPPU : Dec-17, May-19, End Sem, Marks 8]

Ans. :

Sr. No.	Persistent HTTP	Non-persistent HTTP
1.	Persistent version is 1.1.	Non-persistent HTTP version is 1.0.
2.	It uses one RTT.	It uses two RTT.
3.	TCP connection is not closed.	TCP connection is closed after every request-response.
4.	Client make multiple request over the same TCP connection.	Client make multiple request over the multiple TCP connection.
5.	It is default mode.	It is not default mode.
6.	Request methods are GET, HEAD, POST, PUT, DELETE, TRACE and OPTIONS.	Request methods used are GET, POST and HEAD.

Also refer Q.5.

Q.7 Compare the salient features of HTTP and FTP.

Ans. : Comparison of salient features of HTTP and FTP

HTTP	FTP
Retrieve and view web pages	Copy files from client to server or from server to client

The "well known" TCP port for HTTP servers is port 80. Other ports can be used as well.	FTP uses TCP port 20 and port 21.
HTTP protocol is stateless.	The FTP protocol is stateful.
No built-in security mechanisms	It provides security mechanisms.
HTTP is simpler than FTP because it uses one TCP port.	FTP uses two TCP port : One data and one for control.

Q.8 I was downloading an image image1.jpg using the following URL on 2nd november, 2015 : http://www.stockphoto.com/images/image1.gif. Show HTTP request and response messages for getting the image first time.

☞ [SPPU : April-17, In Sem, Marks 5]

Ans. :

1. HTTP Request Message :

GET http://www.stockphoto.com/images/image1.gif HTTP/1.1

Host : www.someschool.edu

User-agent : Mozilla/6.0

Connection : close

2. HTTP Response Message

HTTP/1.1 200 OK

Connection close

Date : 2 November 2015 08:30:52 GMT

Server : Apache/1.3.0 (Unix)

Connection : Close

Expires : 2 November, 2015 15:31:25 GMT

Cache-Control : Max-age = 3600, public

Q.9 Browsers have a in built caching mechanism for a better user experience. How do websites indicate if a web resource needs to be cached or not ? Show HTTP messages in transit for both scenarios.

☞ [SPPU : Dec-17, May-18, End Sem, Marks 8]

Ans. : Caching or temporarily storing content from previous requests, is part of the core content delivery strategy implemented within the HTTP protocol.

- Components throughout the delivery path can all cache items to speed up subsequent requests, subject to the caching policies declared for the content.
- Caches are found at every level of a content's journey from the original server to the browser.
- Web browsers themselves maintain a small cache. Typically, the browser sets a policy that dictates the most important items to cache. This may be user-specific content or content deemed expensive to download and likely to be requested again.
- HTTP response message typically contain a last-modified header with the absolute time of the web resource e.g. an image file.
- Also optionally server may indicate an unique identifier e.g. ETag for the web resource.
- Web server's HTTP response indicates a cache-control header which will be cache-control : No-cache to indicate the browser that the web-resource cannot be cached.
- More commonly, these other headers are also added to force uniform no-caching behavior across browsers.

Q.10 Explain various header of HTTP.

Ans. : • Header can be one or more header lines. Each header line is made of a header name, a colon, a space and a header value.

- The header exchange additional information between the client and the server.
- A header line belongs to one of four categories : General header, request header, response header and entity header.
- Fig. Q.10.1 shows the header format.

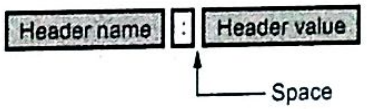


Fig. Q.10.1 Header format

- *General header* includes general information about the message. Request and a response both contains general header.
- *Response header* can be present only in a response message. It specifies the servers configuration and special information about the request.
- Request header can be present only in a request message. It specifies the clients configuration and the client preferred document format.
- *Entity header* gives information about the body of the document. It is mostly present in response messages, some request message, such as POST and PUT methods, that contain a body also use this type of header.
- Fig. Q.10.2 shows the headers.

Status line	HTTP/1.1 300 OK
General headers	Date : Wed, 8 Oct 2014 13:00:13 GMT
	Connection : Close
Response headers	Server : Apache /1.3.27
	Accept ranges : Bytes
Entity headers	Content type : Text/html
	Content length : 200
	Last modified : 2 Oct 2014 13:00:13 GMT
Blank line	
Message body	<html>
	<head>
	<title> Welcome to the India <title>
	<head>
	<body>

Fig. Q.10.2 Response message header

Q.11 Describe briefly HTTP persistent connection.

Ans. : • HTTP 1.1. made persistent connections the default mode.

- The server now keeps the TCP connection open for a certain period of time after sending a response.
- This enables the client to make multiple requests over the same TCP connection and hence avoid the inefficiency and delay of the non-persistent mode.

Types of persistent connections

- There are two versions of persistent connections :
  1. Without pipelining 2. With pipelining

Without pipelining

- The client issues a new request only when the previous response has been received.
- The client experiences one RTT in order to request and receive each of the referenced objects.
- Disadvantage : TCP connection is idle i.e. does nothing while it waits for another request to arrive. This idling wastes server resources.

With pipeling

- Default mode of HTTP 1.1. uses persistent connections with pipeling.
- Client issues a request as soon as it encounters a references. The HTTP client can make back to back requests for the referenced objects.
- It can make a new request before receiving a response to a previous request.
- When the server receives the back-to-back requests, it sends the objects back-to-back.
- It uses only one RTT.
- Pipelined TCP connection remains idle for a smaller fraction of time.
- **Persistent HTTP** connections have a number of **advantages**.
  1. By opening and closing fewer TCP connections, CPU time is saved in routers and hosts.
  2. Requests and responses can be pipelined on a connection.

3. Network congestion is reduced by reducing the number of packets caused by TCP opens.
4. Latency on subsequent requests is reduced.

Proxy server

- HTTP supports the proxy servers. A proxy server is a computer that keeps copies of responds to recent requests.
- The HTTP client sends a request to the proxy server. The proxy server checks its cache.
- If the response is not stored in the cache, the proxy server sends the request to the corresponding server.
- Incoming responses are sent to the proxy server and stored for future requests from other clients.
- The proxy server reduces the load on the original server, decreases traffic and improves latency.
- To use proxy server, the client must be configured to access the proxy instead of the target server.

5.3 : Web Caching

Q.12 What is web caching ? Explain its advantages.

Ans. : • Web caching is the activity of storing data for reuse, such as a copy of a web page served by a web server. Web caching is the storage of Web objects near the user to allow fast access, thus improving the user experience of the web surfer. Examples of some web objects are web pages, images in web pages, etc.

- Web objects can be cached locally on the user's computer or on a server on the Web. There are several types of caches for Web objects :
  1. Browser cache : Browsers' cache web objects on the user's machine. A browser first looks for objects in its cache before requesting them from the website.
  2. Proxy cache : A proxy cache is installed near the web users.

3. Transparent proxy cache : Using a "normal" proxy cache requires configuring the browser appropriately.

Advantages of web caching :

1. Faster delivery of web objects to the end user.
2. Reduces bandwidth needs and cost.
3. Reduces load on the website servers.

5.4 : DNS

Q.13 What is DNS ? Explain in brief hierarchical structure of DNS.

☞ [SPPU : Dec.-15, Marks 6]

Ans. : Domain Name System (DNS)

- The Domain Name System (DNS) is an Internet-wide distributed database that translates betweem domain names and IP addresses.
- The Domain Name System (DNS) is a hierarchical, distributed naming system designed to cope with the problem of explosive growth.
- Domain names are alphanumeric names for IP addresses e.g., www.google.com, ietf.org.

DNS hierarchy of structure

- DNS hierarchy can be represented by a tree.
- Root and top-level domains are administered by an Internet central name registration authority (ICANN)
- Below top-level domain, administration of name space is delegated to organizations.
- Each organization can delegate further.
- Domain names are hierarchical and each part of a domain name is referred to as the root, top level, second level or as a sub-domain. Different levels in DNS hierarchy are listed :

1. Top Level Domains (TLD's)
2. Second Level Domains
3. Sub-Domains
4. Host Name (a resource record)

- Fig. Q.13.1 shows DNS hierarchy.

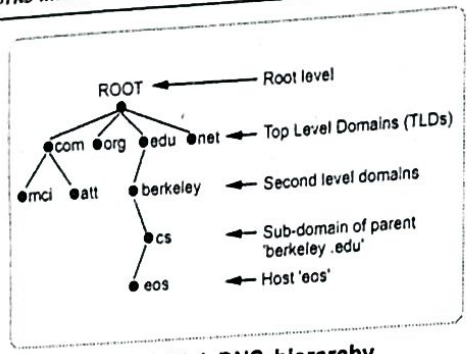


Fig. Q.13.1 DNS hierarchy

- The fully qualified domain name is split into pieces at the dots and the tree is searched starting from the root of the hierarchical tree structure.
- All resolvers start their lookups at the root, therefore the root is represented by a dot and is often assumed to be there, even when not shown.
- The resolver navigates it's way down the tree until it gets to the last, left-most part of the domain name and then looks within that location for the information it needs.
- Information about a host such as its name, its IP address and occasionally even it's function are stored in one or more zone files which together compose a larger zone often referred to as a domain.

Q.14 What is name server ? How resolver looks up a remote name ?

Ans. : • To avoid the problems associated with having only a single source of information, the DNS name space is divided into non-overlapping **zones**. When a resolver has a query about a domain name, it passes the query to one of the local name servers. If the domain being sought falls under the jurisdiction of the name server, it returns the authoritative resource records.

- An **authoritative record** is one that comes from the authority that manages the record and is thus always correct. Authoritative records are in contrast to cached records, which may be out of data.

Resolver looks up a remote name

- If the domain is remote and no information about the requested domain is available locally, the name server sends a query message to the top level name server for the domain requested.
- Consider the following example of Fig. Q.14.1. A resolver on flits.cs.vu.nl wants to know the IP address of the host india.cs.stes.edu.

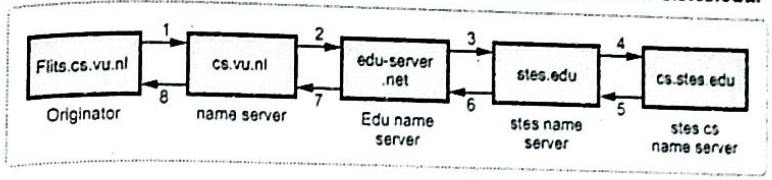


Fig. Q.14.1 Resolver looks up a remote name

Step 1 : It sends a query to the local name server, cs.vu.ne. This query contains the domain name sought, the type (A) and the class (IN).

Step 2 : The local name server has never had a query for this domain before and knows nothing about it. It may ask a few other nearby name servers, but if none of them know, it sends a UDP packet to the server for edu given in its database, edu-server.net.

Step 3 : It is unlikely that this server knows the address of india.cs.stes.edu and probably does not know cs.stes.edu either, but it must know all of its own children, so it forwards the request to the name server for stes.edu.

Step 4 : In turn, this one forwards the request to cs.stes.edu, which must have the authoritative resource records.

Step 5 - 8 : Each request is from a client to a server, the resource record requested works its way back.

- Once these records get back to the cs.vu.nl name server, they will be entered into a cache there, in case they are needed later.

Q.15 Explain DNS request and response message format.

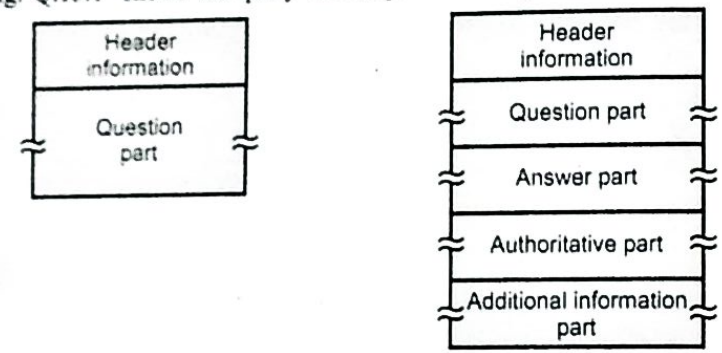
☞ [SPPU: Dec-19, End Sem, Marks 5]

OR Explain DNS message format.

☞ [SPPU : Dec-17, May-18, End Sem, Marks 4]

Ans. : • Messages are sent between domain clients and domain servers with a specific format.

- All messages of this format are used for name resolution and naming queries.
- Question sent by the client and answers provided by the server are included within different fields of the same message.
- DNS has two types of messages : Query and Response. Both types have the same format.
- The query message consists of the header and the question records, the response message consists of a header, question record, answer record, authoritative record and additional records.
- Fig. Q.15.1 shows the query and response messages.



(a) Query (b) Response

Fig. Q.15.1 Query and response message

- Fig. Q.15.2 shows the header format of the DNS. (Refer Fig. Q.15.2 on next page)
- **Identification :** It is 16 bits fields and unique value used by the client to match responses to queries.
- **Flags :** It is the collection of subfields that define the type of messages and type of the answers requested and so on.
- Number of question record contains the number of queries in the question section of the message.

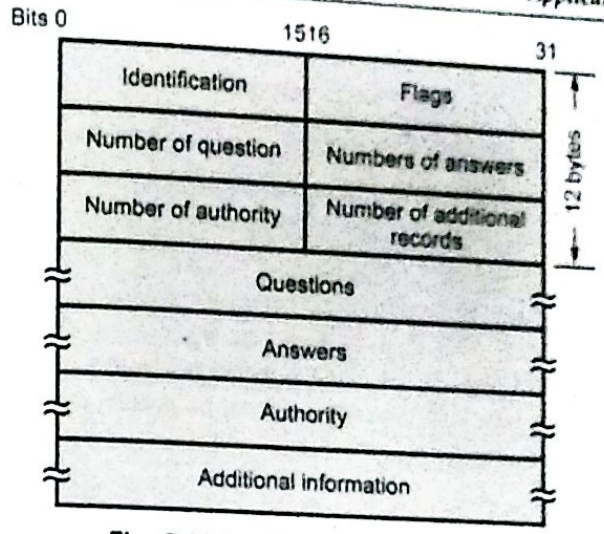


Fig. Q.15.2 General format of DNS

- Number of answer record contains the number of answer records in the answer section of the response message.
- Number of authority record contains the number of authority records in the authoritative section of the response message.
- Number of additional records contains the number of additional records in the additional section of the response message. The message has a fixed 12-byte header followed by 4 variable length fields. The identification field is set by client and returned by the server. It lets the client, match responses to requests.
- Fig. Q.15.3 shows flag fields in DNS header.

	QR	Opcode	AA	TC	RD	RA	Zero	r code
Bit	1	4	1	1	1	1	3	4

Fig. Q.15.3 Flags field in the DNS header

- The flags field is divided into 8 parts.

QR = 0 For message is a query

= 1 It is response

Opcode = 0 Standard query

= 1 Inverse query

= 2 Server status request

AA = Authoritative answer

TC = Truncated

RD = Recursive query

RA = Recursion available

r code = Return code

- RD field is 1-bit and can be set in a query and is then returned in the response. This flag tells the name server to handle the query itself, called a recursive query.
- RA is a 1-bit field and set to 1 in the response if the server support recursion. There is a 3-bit field that must be zero.
- r code is a 4-bit field. The common value are 0 for no error and 3 for name error. A name error is returned only from an authoritative name server and means the domain name specified in the query does not exist.
- The next four 16-bit fields specify the number of entries in the four variable length fields that complete the record.

Q.16 What is DNS ? Explain its various resource records with one example. [SPPU : Dec-18, May-19, End Sem, Marks 8]

Ans. : • Different types of resource records are used in DNS. An IP address has a type of A and PTR means pointer query.

- There are about 20 different types of resource records available. Some PR are listed below.

1) A = It defines an IP address. It is stored as a 32-bit binary value.
2) CNAME = "Canonical name". It is represented as a domain name.
3) HINFO = Host information, two arbitrary character strings specifying the CPU and operating system (OS).
4) MX = Mail exchange records. It provide domain willing to accept e-mail.
5) PTR = Pointer record used for pointer queries. The IP address is represented as a domain name in the in-addr.arpa domain.

6) NS = Name Server record. These specify the authoritative name server for a domain. They are represented as domain names.

Also refer Q.13.

Q.17 What is LDAP ? Explain.

Ans. : • LDAP is Lightweight Directory Access Protocol. It provides X-500 features. LDAP is an applicaion-level protocol that is implemented directly on top of TCP.

- It stores entries, which is similar to objects. Each entry must have a distinguished name, which un-equally identifies the entry. Entries can also have attributes.
- LDAP provides binary, string and time types. It allows the defination of object classes with attribute name of types. Entries are organized into a directory information tree, according to their distinguished names.
- LDAP defines a network protocol for carrying out data definition and manipulation.
- LDAP has been widely adopted, particularly for internet directory services. It provides secured access to directory data through authentication.

5.5 : Email : SMTP, MIME, POP3

Q.18 Explain email function and services in brief.

Ans. : Functions of E-mail : • E-mail system support five basic functions. They are as follows -

1. Composition 2. Transfer 3. Reporting
4. Displaying 5. Disposition

1. **Composition :** It is a process of creating messages and answers. Any text editor can be used for the body of the message. When answering a message, the e-mail system can extract the originator's address from the incoming e-mail.
2. **Transfer :** It is moving messages from the originator to the receiver.
3. **Reporting :** It inform the originator what happened to the message. Whether, email is delivered or not delivered.
4. **Displaying :** Display is required for reading the email.

5. **Disposition** is the last step and related what the receiver does with the message after receiving it. It may be read and save or delete or forward the message.

Q.19 Write short note on :

i) MIME ii) SMTP

[SPPU : Dec-17,18,19, May-18, End Sem, Marks 6]

Ans. : i) MIME : Multipurpose Internet Mail Extensions : • MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.

- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web are encoded using different MIME types.
- Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- Fig. Q.19.1 shows the working of MIME.
- MIME define five headers.
  1. MIME - Version
  2. Content - Type
  3. Content - Transfer - Encoding
  4. Content - Id
  5. Content - Description

Mail Message Header

- From : iresh@e-mail.com
- TO : rupali@sinhgad.edu
- MIME - Version : 1.0
- Content - Type : image/gif

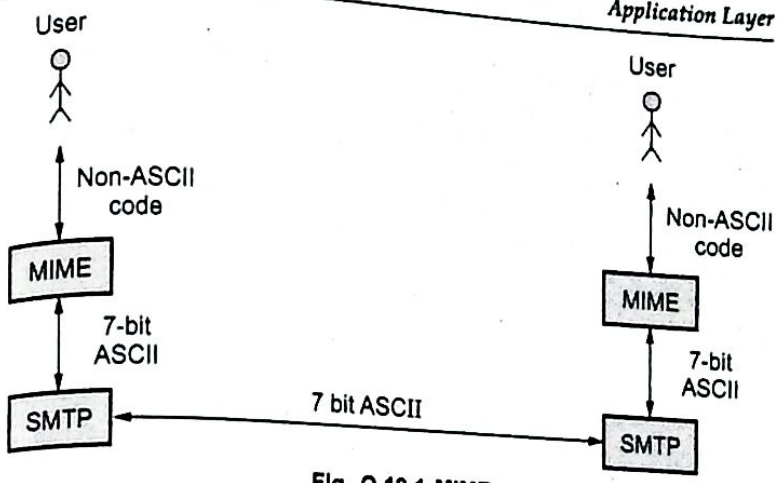


Fig. Q.19.1 MIME

- Content - Transfer - Encoding : base64

..... data for the image .....

....

....

MIME Types and SubTypes

- Each MIME content - type must contain two identifiers :
  - Content type
  - Content subtype
- There are seven standardized content-types that can appear in a MIME content - type declaration.

ii) SMTP : Simple Mail Transfer Protocol :

- SMTP is application layer protocol of TCP/IP model.
- SMTP transfers message from sender's mail servers to the recipients mail servers.
- SMTP interacts with the local mail system and not the user.
- SMTP uses a TCP socket on port 25 to transfer e-mail reliably from client to server.

- E-mail is temporarily stored on the local and eventually transfered directly to receiving server.
- Client / Server interaction follows and commond/reponse paradigm.
  a] Commands are plain ASCII text.
  b] Responses are a status code and an optional phase.
  c] Command and response lines terminated with CRLF.
- Mail client application interacts with a local SMTP server to initiate the delivery of an e-mail message.
- There is an input queue and an output queue at the interface between the local mail system and the client and the server parts of the SMTP.
- The client is concerned with initiating the transfer of mail to another system while server is concerned with receiving mail. Before the e-mail message can be transferred, the application process must be set up a TCP connection to the local SMTP server. The local mail system retains a mailbox for each user into which the user can deposit or retrieve mail. Mail handling system must use a unique addressing system.
- Addressing system used by SMTP consists of two parts : A local part and a global part. The local part is the user name and is unique only within that local mail system. Global part of the address is the domain name. Domain name is identity of the host, must be unique within the total Internet.
- SMTP uses different types of component. They are MIME and POP.

Scenario : Alice sends message to Bob

1. Alice uses User Agent (UA) to compose message and to bob@sinhgad.edu.
2. Alice's UA sends message to her mail server, message placed in message queue.
3. Client side of SMTP opens TCP connection with Bob's mail server.
4. SMTP client sends Alice's message over the TCP connection.
5. Bob's mail server places the message in Bob's mailbox.
6. Bob invokes his user agent to read message.

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

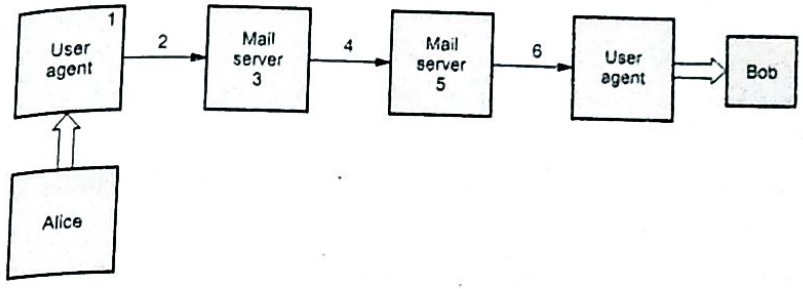


Fig. Q.19.2 Message scenario

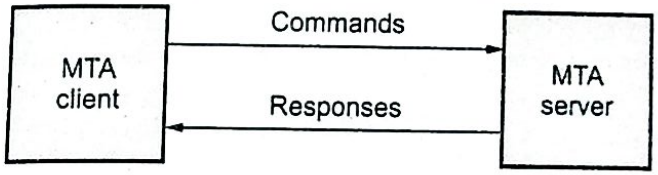


Fig. Q.19.3 Command / Response

- Each command or reply is terminated by a two character end of line token.
- Commands are sent from the client to the server. SMTP defines 14 commands. SMTP commands consist of human readable ASCII strings.

Q.20 Explain working of IMAP. ☞ **[SPPU : Dec-18, 19, End Sem, Marks 5]**

Ans. : • IMAP is the Internet Mail Access Protocol. IMAP4 is more powerful and more complex. IMAP is similar to SMTP.

- It was designed to help the user who uses multiple computers.
- IMAP does not copy e-mail to the user's personal machine because the user may have several.
- An IMAP client connects to a server by using TCP.
- IMAP supports the following modes for accessing e-mail messages :

  i) Offline mode ii) Online mode iii) Disconnected mode

Offline mode : A client periodically connects to the server to download e-mail messages. After downloading, messages are deleted from the server. POP3 support this mode.

Online mode : Client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

Disconnected mode : In this mode, both offline and online modes are supported.

IMAP4 provides the following extra functions :

1. User can check the e-mail header prior to downloading.
2. User can partially download e-mail.
3. A user can create, delete or rename mailboxes on the mail server.

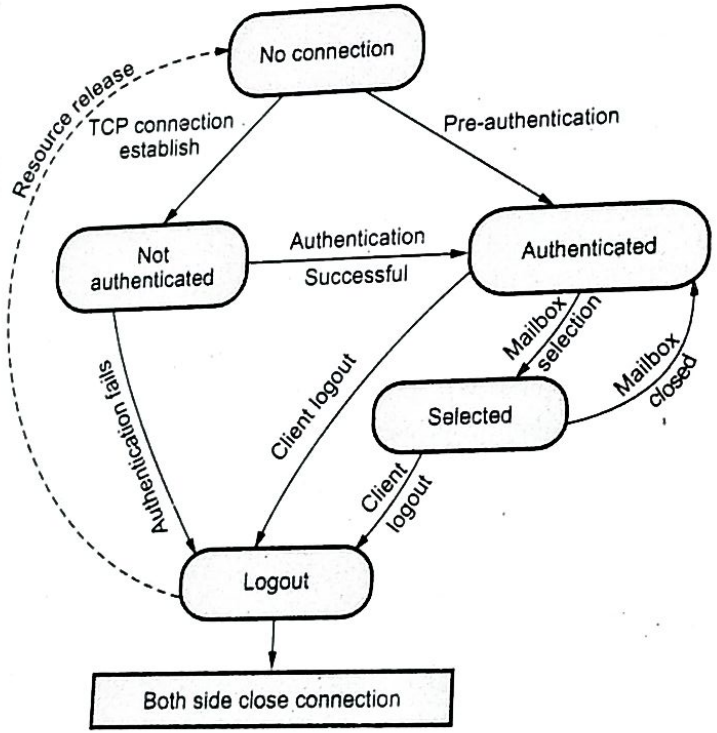


Fig. Q.20.1 IMAP state diagram

4. A user can create a hierarchy of mailboxes in a folder for e-mail storage.
5. User can search the contents of the e-mail for a specific string of characters.

- Fig. Q.20.1 shows IMAP state transition diagram. (Refer Fig. Q.20.1 on previous page)

1. **Not authenticated :** Client provides authentication information to the server.
2. **Authenticated :** Server verify the information and client is now allowed to perform operations on a mailbox.
3. **Selected :** Client is allowed to access of manipulate individual messages within the mailbox.
4. **Logout :** Client send logout command for closing IMAP session.

Q.21 State which transport layer protocol is used by following application layer protocol.
HTTP, FTP, DHCP, DNS, SMTP, TELNET.

☞ **[SPPU : April-15, (In Sem) Marks 3]**

Ans. : Application with application layer protocols is listed below.

Sr. No.	Application	Application layer protocol
1.	Email	SMTP
2.	Web	HTTP
3.	File transfer	FTP
4.	Remote Terminal Access	Telenet
5.	Remote File Server	NSF

Q.22 Compare IMAP and POP3. ☞ **[SPPU : April-15 (In Sem), Marks 4]**

Ans. : Comparison of IMAP and POP3

IMAP	POP3
In IMAP all messages from mail clients and servers are synced with each other.	There is no synchronization
IMAP uses port number 143	POP3 uses port number 110

IMAP protocol allows simultaneous access by multiple clients	POP3 protocol assumes there is only one client connected to the mailbox
The server's store is authoritative	The client's message store is considered authoritative
IMAP supports three modes : Offline mode, Online mode and disconnected mode	POP3 has two modes : Delete mode and the keep mode.

Q.23 Compare file transfer using SMTP and HTTP.

☞ [SPPU : April-15 (In Sem.), Marks 7]

Ans. : Comparison of SMTP and HTTP

SMTP	HTTP
SMTP is push protocol	HTTP is pull protocol
Multiple objects sent in multipart message	Each object encapsulated in its own response message
SMTP uses TCP port number 25	HTTP uses TCP port number 80
SMTP transfers message from sender's mail servers to the recipients mail servers	The set of requests from browsers to servers and the set of responses going back the other way
SMTP interacts with the local mail system and not the user	HTTP interact with users
SMTP is the internet protocol used to transfer electronic mail between computers	HTTP is the internet protocol used to transfer web pages between computers

Q.24 What is user agent and message transfer agent ? Explain.

Ans. : • E-mail system consists of two subsystems : User agent and MTA.

1. **User agent :** It allow user to read and send e-mail. The user agents are local program that provide a command based, menu based or graphical method for interacting with the e-mail system.

- To send an e-mail message, a user must provide the message, the destination address. The destination address should be in proper format and the user agent can deal with destination address.
- Most e-mail system support mailing lists, so that a user can send the same message to a list of people with a single command.
- For reading e-mail, the user agent will look at the user's mail box for incoming e-mail before displaying anything on the screen. It display total number of new mail.

2. **Message transfer agent :** Message Transfer Agent (MTA) move the messages from the source to the destination. MTA are system program that run in the background and move e-mail through the system. After writing the mail, user click of send icon. MTA activates at this time, MTA checks the destination address and transfer the mail to proper destination on the network.

- MTA use different types of protocol for moving the message from source to destination.

1. It must handle temporary failures, if a destination machine is temporarily unavailable, it must spool the message on the local machine for later delivery.
2. MTA must distinguish between local and remote destinations.
3. It may have to deliver copies of a message to several machines.
4. It may allow mixing text, voice and video in a message as well as appending documents and files to a message.

5.6 : FTP

Q.25 Explain FTP. Write any three FTP commands.

☞ [SPPU : May-18,19, End Sem, Marks 8, Dec.-19, End Sem, Marks 5]

Ans. : • Today, transferring files from one computer to another is one of the most common operations on internet.

- Two types of protocols needed for transferring the files on the networks : FTP and TFTP.

- File Transfer Protocol (FTP) is a standard mechanism provided by TCP/IP for copying a file from one computer to another.
- Following problems are associated with file transfer from one machine to another.
  1. Two systems may have different ways to represent text and data.
  2. Two systems may use different file name conventions.
  3. Also, these systems may have different directory structures.
- Therefore, it is necessary for the FTP to solve above mentioned problems in a very simple approach.
- For transferring a file, FTP establishes two connections between the hosts. One connection is used for data transfer and the other connection for control information (commands and responses).
- Separation of connections makes FTP more efficient.
- The data connection needs very complex rules due to the variety of data types transferred; on the other hand, the control connection uses very simple rules of communication.
- FTP uses the services of TCP as its underlying transport protocol.
- It needs two TCP connections.
- The well-known port 21 is used for the control connection and port 20 is used for the data connection.
- The following Fig. Q.25.1 shows the basic model of FTP connection. As shown in figure, the client has three components whereas the server has only two.
- It is clearly shown in Fig. Q.25.1 that the control connection is done between the control processes while the data connection is done between the data transfer processes.
- When a client starts an FTP session, the control connection remains open during the entire interactive session, while the data connection is opened when the user wants to transmit a file and it closes when the file is transferred.

Also refer Q.27.

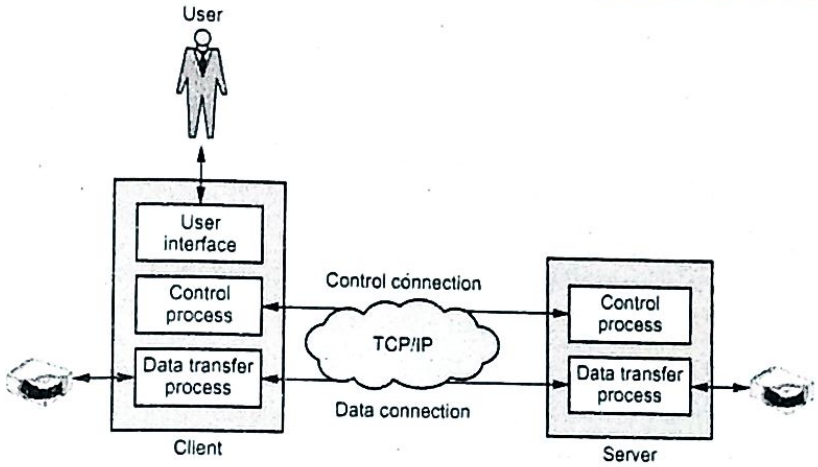


Fig. Q.25.1 FTP

Q.26 When I asked my company admin for some software he asked me to use 'anonymous FTP' and download it ? What is it ? Outline a problem scenario using it. [SPPU : April-16, (In Sem), Marks 5]

Ans. : We can configure FTP servers one of two ways :

i) Private user-only site. Allows only system users to connect via FTP and access their files.

ii) Anonymous. Allows anyone on the network to connect to it and transfer files without having an account.

- An anonymous FTP site is a computer with ftp archives permitting anyone to log on with the username : Anonymous and password : Your e-mail address.
- Assume you are required to download the file ***playgame.txt*** from *dho.cdrom.com/pub/games/*

1. At the command prompt type : ***ftp papa.cdrom.com*** (for stating ftp and connection to the site)

   The system will respond with the message

   >connected to sunsite.cnlab-switch.ch.

   >220 warchive.cdrom.com. FTP server (Version wu-2.4.2(18)

   >Thu oct 27 07:32:12 MET 2011) ready.

>Name (carchive.cdrom.com:usr) :

2. Type *ftp*

   The system will respond with something similar to.

   >331 Guest login ok, send your complete e-mail address as password

   >Password : **(type your email)**

3. After the welcome message that may look something like this.

   230 guest login ok, access restrictions apply.

   Remote system type is UNIX.

   We must now change to the directory "/pub/games"

   Type in ***cd pub*** (it will change to the directory pub), this directory contents downloadable material.

   Lets type ***dir*** to see the list of files in there we should see the directory games in the list.

   drwxr-xr-x 6 731 730 512 Nov 4 05:11 games

   The d in front of the listing tells me it is a directory. If dir does not work we can use the command : *ls-al*

4. Use 'dir' to find the file :

   Type: *dir l**

   to get a listing of all files which start with 'l'.

   You should see :

   -rw-rw-r- 1 2066 ftp-game 134868 Jun 13 2007 playgame.txt

   Because there is no 'd' at the far left, you know that it is a file, not a directory.

   The 134868 is the file size, it is 134,868 byte. It was last modified on the 13th of June 2007.

5. To download, type : *bin*

   This will make your download in 'binary' form

   This mode will always work for all files, whereas the default mode *'ascii'* will only work for text files.

Therefore always make sure you type *'bin'* before you download or you may get garbage!

6. Type : get playgame.txt

   And type 'y' when asked to confirm.

   'playgame' will now download, and will soon be on the computer you ran *'ftp'* from.

7. Alternately, if you want to download multiple files, you could type : *'mget *'*, this would download *all* files in the directory; 'mget l*' would download all files beginning with *'l'*.

8. If you do not wish to confirm each download one by one, type *'prompt'* to turn that off. If you wish to have a download indicator, type *'hash'*.

Q.27 List and explain FTP Commands.

Ans. :

Sr. No.	Command	Meaning
1.	cd	Changes the working directory on the remote host
2.	close	Closes the FTP connection
3.	quit	Quits FTP
4.	pwd	Displays the current working directory on the remote host
5.	dir or ls	Provides a directory listing of the current working directory
6.	help	Displays a list of all client FTP commands
7.	remotehelp	Displays a list of all server FTP commands
8.	type	Allows the user to specify the file type
9.	struct	Specifies the files structure

Q.28 Compare FTP with TELNET.

Ans. :

Sr. No.	FTP	TELNET
1.	FTP is a two-way system - it can be used to copy or move files from a server to a client computer as well as upload or transfer files from a client to a server.	TELNET is two –way system (with authorization) it can be used to copy or moves files from other computer.
2.	FTP systems generally encode and transmit their data in binary sets which allow for faster data transfer.	TELNET while connection client-server communication is non-coded.
3.	Commands : ASCII, Binary, Open, Del and Get.	Commands : Open, Close, Display, Status and Quit.

5.7 : TELNET

Q.29 Explain with diagram TELNET client server interaction. Also explain control characters used to control remote server.

Ans. : TELNET is a TCP applications. It provides the ability to perform remote logons to remote hosts. TELNET operates using a client and server. Fig. Q.29.1 shows TELNET client server interaction schematic.

- The client TELNET protocol is accessed through the local Operating System (OS) either by user or by a user at a terminal. It provides services to enable a user to log on to the operating system of a remote machine, to initiate the running of a program on that machine. All the commands and data entered at the user terminal are passed by the local operating system to the client TELNET process which then passes them, using the reliable stream service provided by TCP, to the correspondent server TELNET. The two TELNET protocols communicate with each other using commands that are encoded in a standard format known as network virtual terminal. The character set used for commands is

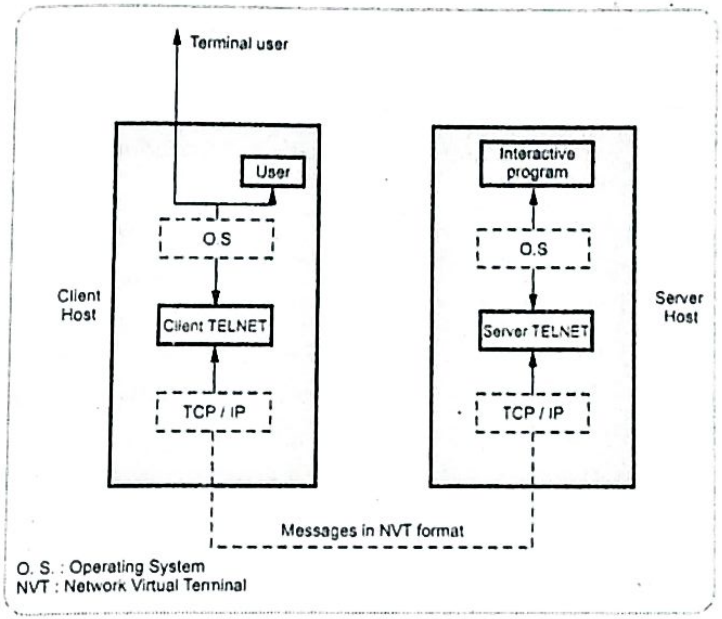


Fig. Q.29.1 TELNET client / server interaction

ASCII. All input and output data relating to an interaction is transferred as ASCII strings. If this is different from the local character set being used, the corresponding TELNET will carry out any necessary mapping functions. Thus, the two TELNET protocol entities also perform the role of the presentation layer in an OSI stack.

- Following are the Telnet commands.

Name	Code	Meaning
EOF	236	End of file
ABORT	238	Abort process
EOR	239	End of record
NOP	241	No operation
Go Ahead	249	The GA signal
IAC	255	Data byte 255

- Control characters used to control remote server in Telnet are as follows :
  1. IP : Interrupt Process which is used to interrupt the program.
  2. AO : Abort Output allows the process to continue without creating output.
  3. AYT : Are You There. It determines if the remote server is running after a long silence from server.
  4. EC : Erase Character. It is used to delete last character.
  5. EL : Erase Line. It is used to erase current line in remote host.

Q.30 What is TELNET ? Explain properties of TELNET ? What are different mode of operation used in TELNET ?

Ans. : • Client-server model can create a mechanism that allows a user to establish a session on the remote machine and then run its application. This application is known as remote login. Telnet is the example of remote login.

- TELNET (terminal network) is a protocol that provides "a general, bi-directional, eight-bit byte oriented communications facility". It is a program that supports the TELNET protocol over TCP. Many application protocols are built upon the TELNET protocol.
- A client program running on the user's machine communicates using the Telnet protocol with a server program running on the remote machine. The Telnet client program performs two important functions :
  1. Interacting with the user terminal on the local host.
  2. Exchanging messages with the Telnet server.
- The client connects to port 23 on the remote machine, which is the port number reserved for Telnet servers. The TCP connection persists for the duration of the login session. The client and the server maintain the connection, even when the user interrupts the transfer of data, for example by hitting cntl-C.
- Since Telnet is designed to work over two hosts on different platforms, the protocol assumes that the two hosts run a Network Virtual Terminal (NVT). The TCP connection is set up across these two NVT terminals.

The NVT is a very simple character device with a keyboard and a printer, data typed by the user on the keyboard is translated by the client software into NVT format and sent via its NVT terminal to the server, and data received in NVT format from the server is translated by the client into the local machine format and output to the printer.

NVT uses two types of set in TELNET :

1. Data character : It has 8 bit in which lowest bit is set as ASCII and highest order bit is 0.
2. Control character : It uses 8 bit character set in which highest order bit is set and lowest order bit is 1.

- TELNET has the following properties :
  1. Client programs are built to use the standard client/server interface without knowing the details of server programs.
  2. A client and server can negotiate data format options.
  3. Once a connection is established through TELNET, both ends of the connection are treated symmetrically.

Different modes of operation in Telnet

1. **Default mode :** It is half duplex and has become obsolete. Echoing is done by client.
2. **Character mode :** Server echoes the character back to screen and it can be delayed if transmission time is low. It also creates overhead for network.
3. **Line mode :** Line editing, Line erasing, Character erasing is done by client. It is full duplex mode.

5.8 : DHCP

Q.31 Why we need DHCP ? Explain in details.

☞ [SPPU : May-19, End Sem, Marks 8, Dec-19, End Sem, Marks 5]

Ans. : • The Bootstrap Protocol (BOOTP) is a static configuration protocol. Each client has a permanent network connection.

- When a client requests its IP address, BOOTP server checks a table that matches the physical address of the client with its IP address. The binding is predefined,

- If the client moves from one network to another then its creates a problem. BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the system administrator. If there is a change in a physical or IP addresses, the administrator needs to manually enter the changes.
- So, to remove the limitations of BOOTP, Dynamic Host Configuration Protocol (DHCP) is used.
- DHCP does not require an administrator to add entry for each connection to the database. DHCP provides a mechanism that allows a computer to join a new network and obtain an IP address without manual intervention. The DHCP work like plug and play networking.
- The DHCP provides static and dynamic address allocation. Static addresses are created manually whereas dynamic addresses are created automatically.
- **Static address allocation** : DHCP is backward compatible with BOOTP, which means a computer running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.
- **Dynamic address allocation** : DHCP has a pool of available IP addresses. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available IP addresses (unused addresses) and assigns an IP address for a negotiable period of time.
- When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned. On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.
- DHCP provides temporary IP addresses for a limited time. The addresses assigned from the pool are temporary addresses. The DHCP server issues a lease for a specific time. When the lease is expired, the

client must either stop using the IP address or renew the lease. The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the address.

Q.32 Write short note on DHCP.

[SPPU : May-18, Dec.-17,18, End Sem, Marks 3]

Ans. : • DHCP (Dynamic Host Configuration Protocol) is a communications protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network.

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details.
- DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.
- DHCP works on a client-server model. Being a protocol, it has it's own set of messages that are exchanged between client and server.

DHCP server

- A DHCP Server assigns IP addresses to client computers. This is very often used in enterprise networks to reduce configuration efforts. All IP addresses of all computers are stored in a database that resides on a server machine.

5.9 : SNMP

Q.33 What is SNMP ? Explain management components of SNMP.

Ans. : • Network management is a technique for monitoring, testing, configuring, and troubleshooting network components so that it is used to meet a set of requirements defined by an organization.

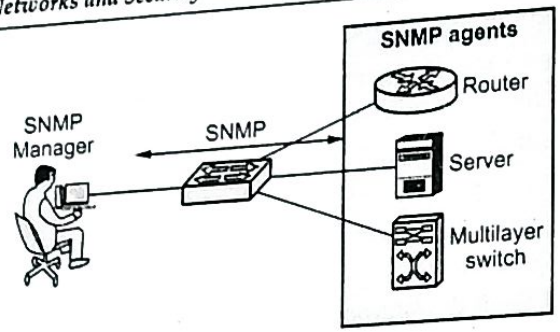


Fig. Q.33.1 SNMP concept

- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers.
- SNMP uses the concept of manager and agent. The manager (sometimes called Network Management System) can be any machine that can send query requests to SNMP agents usually routers or servers with the correct credentials.
- SNMP is an application-level protocol in which a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- A manager is usually a host that runs the SNMP client program and an agent is usually a router that runs the SNMP server program.
- The agent keeps the information in a database such as the number of packets received and forwarded. The manager can access this database.

Management components

- To do management tasks, SNMP uses other two protocols : Structure of Management Information (SMI) and Management Information Base (MIB).

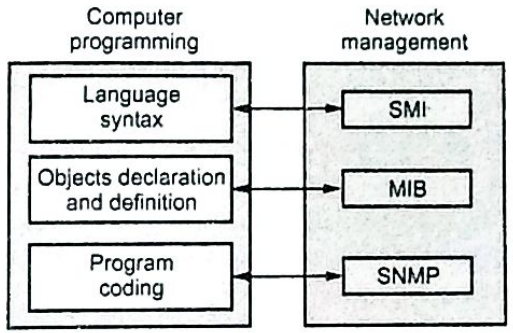


Fig. Q.33.2 Management components

- The network management components on the Internet are : SNMP, SMI, and MIB.
- **SNMP** defines the format of the packet to be sent from a manager to an agent and vice versa. It reads and changes the status of objects (values of variables) in SNMP packets.
- **SMI** defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.
- **MIB** creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.
- The above three network management components are exactly similar to what we need when we write a program in a computer language to solve a problem is as follows.
- Before we write a program, the syntax of the any language (such as C++ or Java) must be predefined. The language defines the structure of variables and how the variables assigned named. The language also defines the type of data to be used. In programming the rules are defined by the syntax of the language. In network management the rules are defined by SMI.
- Any computer languages require that objects be declared and defined in each specific format. For example, if a program has two variables (an integer named increment and an array named grades of type char), they

must be declared at the beginning of the program. MIB does this task in network management. MIB names each object and defines the type of the objects.

- After declaration in programming, the program needs to write statements to store values in the variables and change them whenever needed. SNMP does this task in network management. SNMP stores, changes, and interprets the values of objects already declared by MIB according to the rules defined by SMI.

Q.34 Describe SNMP messages.

Ans. :

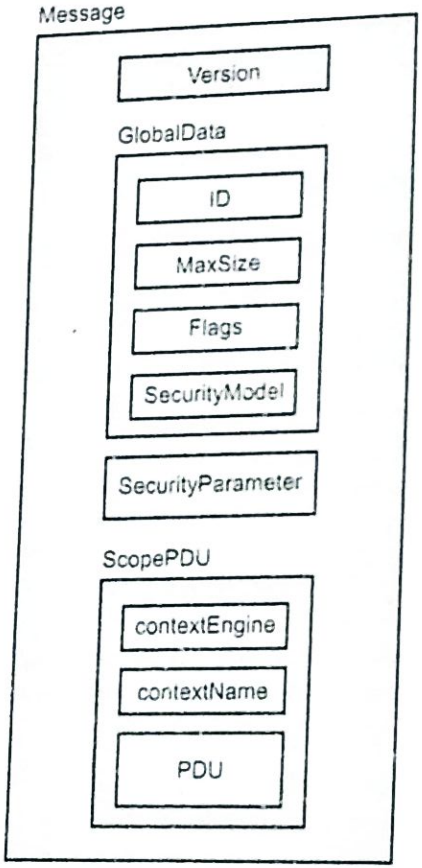


Fig. Q.34.1 SNMP messages

- SNMP does not send only a PDU but it attach the PDU in a message. SNMP message has four elements : Version, GlobalData, SecurityParameters, and ScopePDU.
- The Version field is an INTEGER data type that defines the current version.
- The GlobalData field is a sequence having four elements of simple data type : ID, Max-Size, Flags, and SecurityModel.
- Security parameter depends on the type of security used in current version3 of SNMP.
- The ScopePDU element contains two simple data type and the actual PDU.

END...

Unit VI

6 Security

6.1 : Introduction

Q.1 What is NIST definition of computer security ?

Ans. : • The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources.

Q.2 What is computer security and network security ?

Ans. : • Computer security is a generic name for the collection of tools designed to protect data and to thwart hackers

• Network Security : It measures to protect data during their transmission.

Q.3 What is the need for security ?

Ans. : Now a day, protection is easier because many factors working against the potential criminal. Very sophisticated alarm and camera systems silently protect secure places like banks.

- Traditionally information security provided by physical i.e. rugged filing cabinets with locks and administrative mechanisms i.e. personnel screening procedures during hiring process.
- Asset protection systems are designed to recover stolen cash and high value assets, apprehend criminals and deter crime. The system has the capacity to track, protect and manage critical assets in real-time.
- The techniques of criminal investigation have become so effective that a person can be identified by genetic material, voice, retinal pattern, fingerprints etc.
- Use of networks and communications links requires measures to protect data during transmission.

- **Data security** is the science and study of methods of protecting data from unauthorized disclosure and modification.
- Data and information security is about enabling collaboration while managing risk with an approach that balances availability versus the confidentiality of data.
- **Computer security :** Generic name for the collection of tools designed to protect data and to hackers.
- **Network security :** Measures to protect data during their transmission.
- **Internet security :** Measures to protect data during their transmission over a collection of interconnected networks.

Protecting valuables

- Following are certain aspects for the need of security :
  1. Increasing threat of attacks.
  2. Fast growth of computer networking for information sharing.
  3. Availability of number of tools and resources on internet.
  4. Lack of specialized resources that may be allotted for securing system.

Q.4 What are the principles of security ?

Ans. : • Principles of security are confidentiality, authentication, integrity, availability, non-repudiation and access control.

Q.5 List and explain security goals.

Ans. : Various elements of information security are :

1. Confidentiality 2. Integrity 3. Availability

Security goals are as follows :

1. **Confidentiality** refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones. Sensitive information should be kept secret from individuals who are not authorized to see the information.
2. **Integrity** ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential

communication, but may have the ability to change the information being transmitted.

3. **Availability** refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.

Q.6 Explain the terminologies used in encryption.

Ans. : • Basic terminology used for security purposes are as follows :

a. **Cryptography :** The art or science encompassing the principles and methods of transforming an plaintext message into one that is unintelligible and then retransforming that message back to its original form.

b. **Plaintext :** The original message.

c. **Ciphertext :** The transformed message produced as output, It depends on the plaintext and key.

d. **Cipher :** An algorithm for transforming plaintext message into one that is unintelligible by transposition and/or substitution methods.

e. **Key :** Some critical information used by the cipher, known only to the sender and receiver.

f. **Encipher (encode) :** The process of converting plaintext to ciphertext using a cipher and a key.

g. **Decipher (decode) :** The process of converting ciphertext back into plaintext using a cipher and a key.

h. **Cryptanalysis :** The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **code-breaking.** Cryptanalysis is to break an encryption. Cryptanalyst can do any or all of the three different things :

1. Attempt to break a single message.
2. Attempt to recognize patterns in encrypted messages, in order to be able to break subsequent ones by applying a strainghtforward decryption algorithm.

3. Attempt to find general weakness in an encryption algorithm, without necessarily having intercepted any messages.

i. **Cryptology :** Both cryptography and cryptanalysis.

j. **Code :** An algorithm for transforming an plaintext message into an unintelligible one using a code-book.

6.2 : Security Services

Q.7 Give various security services.

Ans. : • Security services into five different categories : Authentication, Access control, Data confidentiality, Data integrity and Non-repudiation.

Q.8 List and briefly define categories of security services and attacks.

Ans. : Security services are as follows :

1. Authentication
2. Access control
3. Data confidentiality
4. Data integrity
5. Nonrepudiation

• X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

1. **Authentication** is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.
2. **Access control :** It is the ability to limit and control the access to host systems and applications via communications links. This service controls who can have access to a resource.
3. **Data confidentiality :** Confidentiality hides the information or resources. It is the protection of transmitted data from passive attacks.
4. **Data integrity :** Integrity can apply to a stream of messages a single message or selected fields within a message. Modification causes loss of message integrity.
5. **Nonrepudiation :** Nonrepudiation prevents either sender or receiver from denying a transmitted message. When a message is sent, the receiver can prove that the alleged sender in fact sent the message.

6.3 : Types of Attacks

Q.9 Define an attack.

Ans. : • An attack on system security that derives from an intelligent threat : that is an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Q.10 What are the types of security attacks ?

Ans. :

- Types of security attacks are passive attacks and active attacks.
- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks cannot be prevented easily.

Q.11 Discuss in detail about various types of security attacks with neat diagrams.

Ans. : Passive attack

- Passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- The attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data.
- **Passive attacks** are of two types :
  1. Release of message contents
  2. Traffic analysis
- **Release of message content** is shown in Fig. Q.11.1. A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information we would like to prevent an opponent from learning the content of these transmissions.

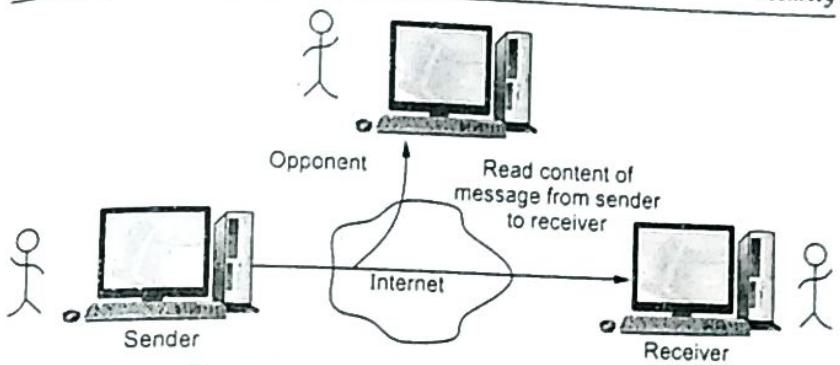


Fig. Q.11.1 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. Q.11.2 shows the traffic analysis.

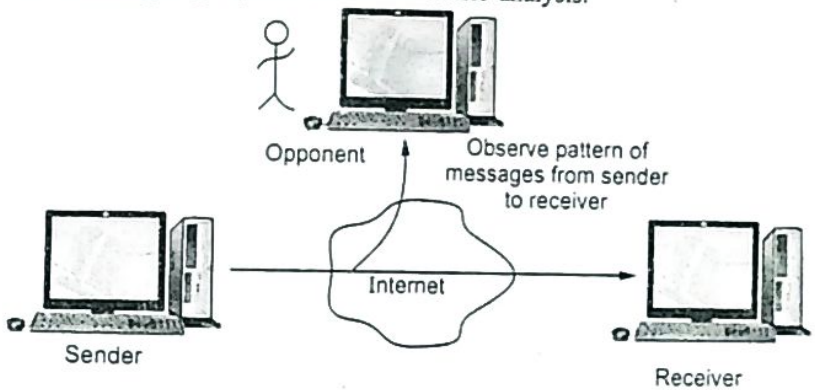


Fig. Q.11.2 Traffic analysis

- Passive attacks are very difficult to detect because they do not involve any alternation of data. It is feasible to prevent the success of attack, usually by means of encryption.

Active attack

- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.
- Active attacks can be subdivided into four types :
  1. Masquerade
  2. Replay
  3. Modification of message
  4. Denial of service

1. Masquerade

- It takes place when one entity pretends to be a different entity. Fig. Q.11.3 shows masquerade.

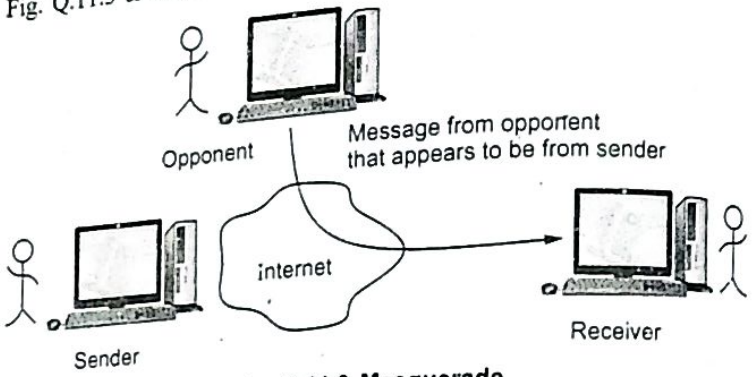


Fig. Q.11.3 Masquerade

- **For example :** Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- **Interruption** attacks are called as masquerade attacks.

2. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Fig. Q.11.4 shows replay attack.

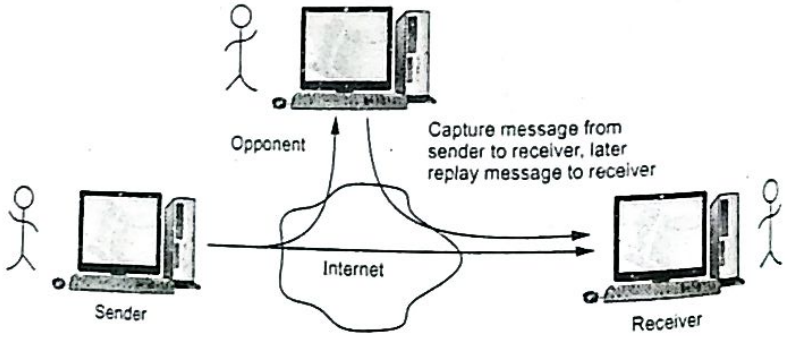


Fig. Q.11.4 Replay

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. Q.11.5 shows the modification of message.

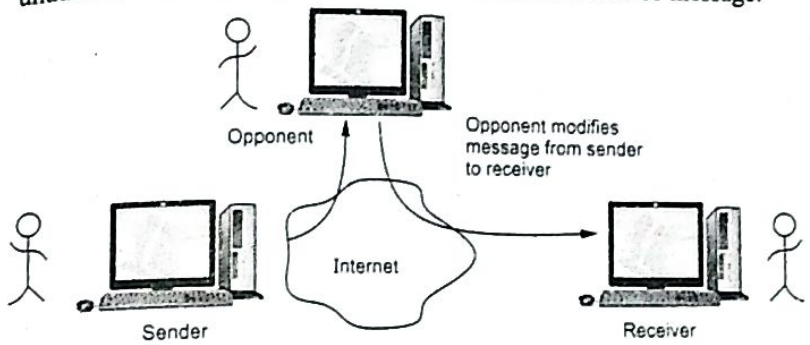


Fig. Q.11.5 Modification of message

- For example, a message meaning "Allow Rupali Dhotre to read confidential file accounts " is modified to mean "Allow Mahesh Awati to read confidential file accounts".

4. Denial of service

- Fabrication causes Denial Of Service (DOS) attacks.
- DOS prevents the normal use or management of communications facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

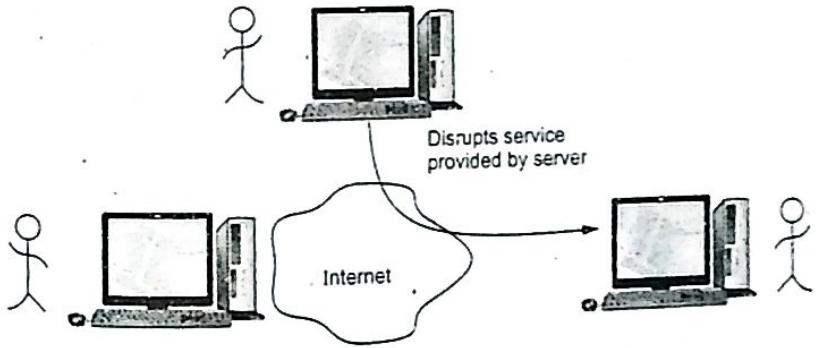


Fig. Q.11.6 Denial of service

- Fig. Q.11.6 shows denial of service attack.
- It is difficult to prevent active attack because of the wide variety of potential physical, software and network vulnerabilities.
- The first type of DOS attacks were single source attacks, meaning that a single system was used to attack another system and cause something on that system to fail. SYN flood is the most widely used DOS attack.
- Fig. Q.11.7 shows the SYN flood DOS attack.

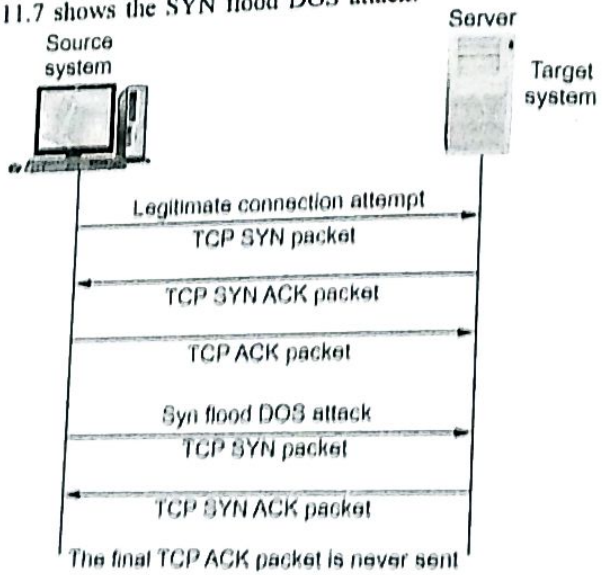


Fig. Q.11.7 SYN flood DOS attack

- Source system sends a large number of TCP SYN packets to the target system. The SYN packets are used to begin a new TCP connection.
- When the target receives a SYN packet, it replies with TCP SYN ACK packet, which acknowledges the SYN packet and sends connection setup information back to the source of the SYN.
- The target also places the new connection information into a pending connection buffer.
- For a real TCP connection, the source would send a final TCP ACK packet when it receives the SYN ACK.

- However, for this attack, the source ignores the SYN ACK and continues to send SYN packets. Eventually, the target's pending connection buffer fills up and it can no longer respond to new connection requests.

Q.12 Compare passive and active attack.

Ans. :

Sr. No.	Passive attacks	Active attacks
1.	Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.	Active attacks involve some modification of the data stream or the creation of a false stream.
2.	**Types :** Release of message contents and traffic analysis	**Types :** Masquerade, replay, modification of message and denial of service.
3.	Very difficult to detect.	Easy to detect.
4.	The emphasis in dealing with passive attacks is on prevention rather than detection.	It is quite difficult to prevent active attacks absolutely.
5.	It does not affect the system.	It affects the system.

6.4 : X.800 Security

Q.13 Explain OSI security architecture.

Ans. : • X.800 recommends sending architecture for OSI. The OSI security architecture define systematic way to asses security needs of on organization and help them to choose various security products and fields.

- The OSI security architecture mainly focuses on :

a) Security attack :

- Any action which comprises the organizaion secured information.

b) **Security mechanism :**
- A process designed to detect, prevent receiver from a security attack.

c) **Security service :**
- The security service are intended to counter security attack by making use of the one or more security mechanism.

6.5 : Security Policy and Mechanism

Q.14 What is a security mechanism ?

Ans. : A security mechanism is any process that is designed to detect, prevent or recover from a security attack.

Q.15 What are security mechanisms ? Explain.

Ans. : Various security mechanism are encipherment, digital signature, access control, data integrity, traffic padding, notarization, event detection, security recovery, security label etc.

Q.16 What are the various security mechanisms ?

Ans. : • X.800 defined security mechanisms as follows

1. **Specific security mechanisms :** May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
   a. **Encipherment :** The use of mathematical algorithms to transform data into a form that is not readily intelligible.
   b. **Digital signature :** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
   c. **Access control :** A variety of mechanisms that enforce access rights to resources.
   d. **Data integrity :** A variety of mechanisms used to ensure the integrity of a data unit or stream of data units.
   e. **Authentication exchange :** A mechanism intended to ensure the identity of an entity by means of information exchange.

   f. **Traffic padding :** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
   g. **Notarization :** The use of a trusted third party to assure certain properties of a data exchange.

2. **Pervasive security mechanisms :** Mechanisms that are not specific to any particular OSI security service or protocol layer.
   a. **Trusted functionality :** That which is perceived to be correct with respect to some criteria.
   b. **Event detection :** Detection of security relevant events.
   c. **Security label :** The marking bound to resource that names or designates the security attributes of that resource
   d. **Security recovery :** Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

6.6 : Operational Model of Network Security

Q.17 Explain the network security model.

Ans. : A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols by the two principals

Q.18 What is traffic Padding ? What is its purpose ?

Ans. : • The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

- Traffic padding produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated.
- When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted.
- This makes it impossible for an attacker to distinguish between true data flow and padding and therefore impossible to deduce the amount of traffic.

- Traffic padding is essentially a link encryption function. If only end-to-end encryption is employed, then the measures available to the defender are more limited.
- If encryption is implemented at the application layer, then an opponent can determine transport layer, network-layer addresses and traffic patterns which remain accessible

Q.19 Explain the model of network security.

Ans. : A message is to be transferred from source to destination across some sort of internet. Both the sides must cooperate for the exchange of the data.

- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components :
  1. A security related transformation on the information to be sent.
  2. Some secret information shared by the two principles, it is hoped, unknown to the opponent.
- Fig. Q.19.1 shows the network security model. (See Fig. Q.19.1 on next page)
- A trusted third party is needed to achieve secure transmission.
- Basic tasks in designing a particular security service :
  1. Design an algorithm for performing the security related transformation.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.
  4. Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service.

6.7 : Symmetric Key Cryptography

Q.20 Define symmetric encryption.

Ans. : In symmetric encryption, sender and receiver use same key for encryption and decryption.

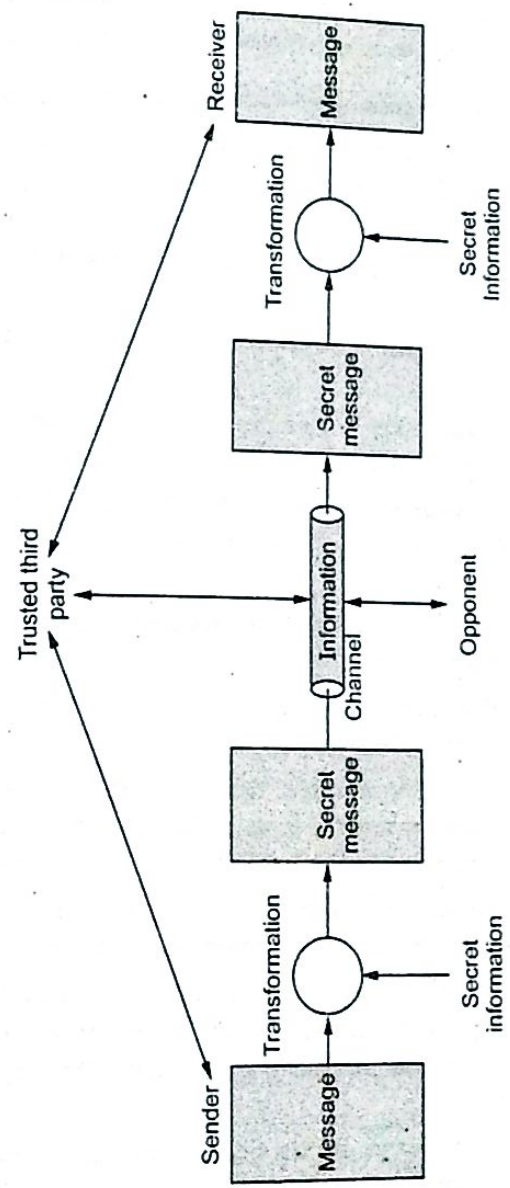


Fig. Q.19.1 Network security model

Q.23 Define cryptanalysis.

Ans. : • Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis

Q.24 Explain advantages and disadvantages of symmetric key cryptography.

Ans. : Advantages of symmetric-key cryptography

1. High rates of data throughput.
2. Keys for symmetric-key ciphers are relatively short.
3. Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms (i.e. pseudorandom number generators).
4. Symmetric-key ciphers can be composed to produce stronger ciphers.
5. Symmetric-key encryption is perceived to have an extensive history.

Disadvantages of symmetric-key cryptography

1. Key must remain secret at both ends.
2. In large networks, there are many keys pairs to be managed
3. Sound cryptographic practices dictates that the key be changed frequently
4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys or the use of third trusted parties.

Q.25 What is DES ?

Ans. : DES is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 46 in 1977, as the federal government approved encryption algorithm for sensitive but non-classified information. DES utilizes a 56-bit key. This key size is vulnerable to a brute force attack using current technology.

Q.26 Write down the purpose of the S-boxes in DES.

Ans. : In S-box, each row defines a general reversible substitution. It consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

Q.27 Write about strength of DES algorithm.

Ans. :

1. As 56-bit keys are used there are 70 quadrillion possible key values and hence a specific key cannot be identified easily.

2. As the length of the key is increased the security provided by the algorithm also increases.
3. The security of the DES algorithm resides in the key.

Q.28 Explain DES algorithm with suitable examples. Discuss its advantages and limitations.

Ans. : DES algorithm : • DES Encryption Standard (DES) is a **symmetric key block cipher** published by the National Institute of Standards and Technology (NIST).

- It encrypts data in 64-bit block.
- DES is symmetric key algorithm : The same algorithm and key is used for both encryption and decryption.
- Key size is 56-bit.
- The encryption process is made of two permutations i.e. P-boxes, which is called initial and final permutation.
- DES uses both transposition and substitution and for that reason is sometimes referred to as a **product cipher**. Its input, output and key are each 64-bits long. The sets of 64-bits are referred to as **blocks**.
- The cipher consists of 16 rounds or iterations. Each rounds uses a separate key of 48-bits.
- Fig. Q.28.1 shows DES encryption algorithm. First, the 64-bit plaintext passes through an Initial Permutation (IP) that rearranges the bits to produce the permuted input.
- Then there is a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.
- The output of the sixteenth round consists of 64-bits that are a function of the input plaintext and the key.
- The left and right halves of the output are swapped to produce the pre-output. At last, the pre-output is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

Initial permutation

- Table shows the initial permutation and its inverse. The input to a table consist of 64-bits numbered from 1 to 64.

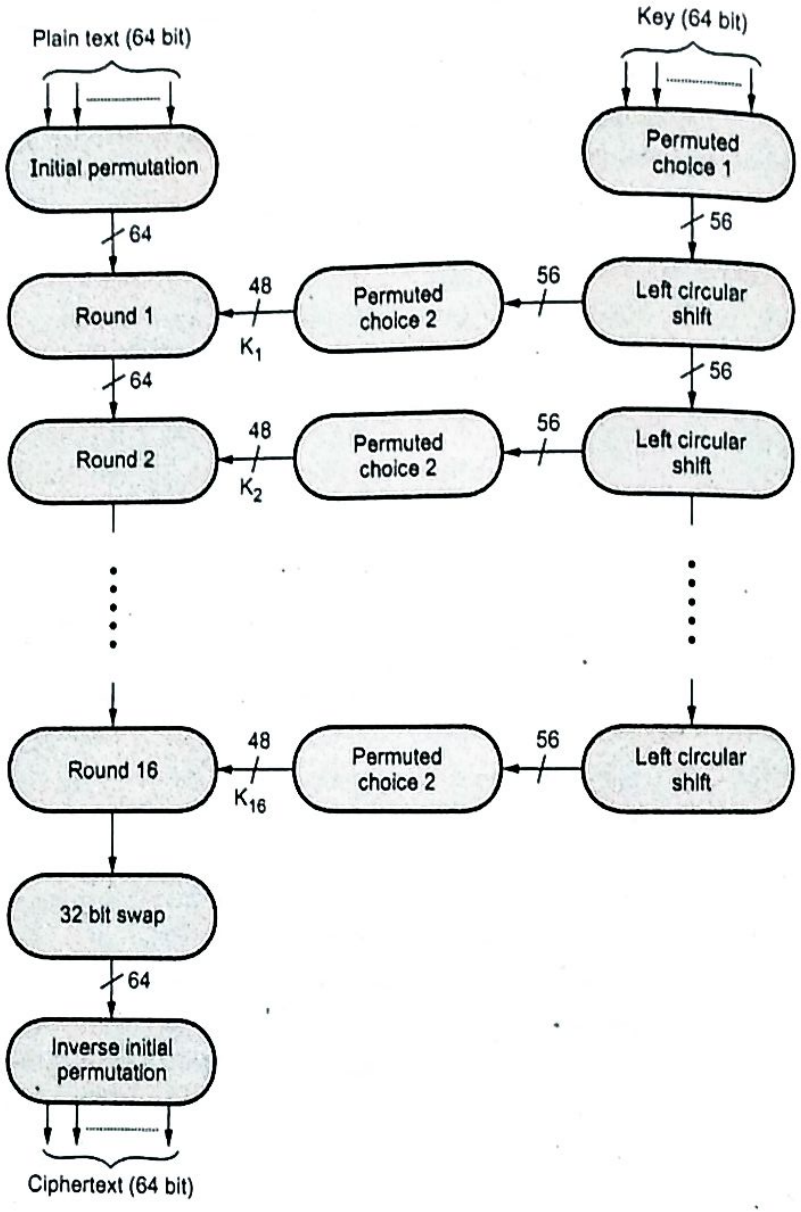


Fig. Q.28.1 DES encryption algorithm

- The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the positon of a numbered input bit in the output, which also consists of 64-bits.

Initial Permutation (IP) table

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	2.1	13	5
63	55	47	39	31	23	15	7

Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES Advantages : Refer Q.24.

DES limitations :

1. As it is a symmetric algorithm both sender and receiver must have same key, there is a possibility that the key is intercepted.
2. The design of S boxes makes it susceptible to linear cryptanalysis attack.
3. It is susceptible to differential cryptanalysis attack and brute force attack taking advantage of which DES crackers have been designed.
4. It has certain weak keys which generate the same key for all cycles of the algorithm like when all key bits are either 0s or 1s or if one half of the key bits are 0s or 1s. They are 0000000 0000000, 0000000 ffffff, ffffff 0000000, ffffff ffffff.
5. Some initial keys produce only two subkeys while some produce only four. They are called possible weak keys.

Possible techniques for improving DES

- Multiple enciphering with DES
- Extending DES to 128-bit data paths and 112-bit keys
- Extending the key expansion calculation.

Q.29 What is AES ? Explain its characteristics.

Ans. : AES

- Advanced Encryption Standard (AES) is a symmetric key block cipher published by the NIST in December 2001.
- AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bits.
- The key size can be 128,192 or 256-bits. It depends on number of rounds.
- The number of rounds : 10 rounds for 128-bits, 12 rounds for 192-bits and 14 rounds for 256-bits.

Characteristics :

1. Resistance against all known attacks.
2. Speed and code compactness on a wide range of platforms.
3. Design simplicity.

- For 128-bits AES, each round contains four steps :
  i. Byte substitution ii. Row shift
  iii. Column mixing iv. Round key addition
- The input to the encryption and decryption algorithms is a single 128-bit block. The block is represented as a row of matrix of 16 bytes.
- AES use several rounds in which each round is made of several stages. Data block is transformed from one stage to another.
- Data block is referred to as state. Block is copied into state array which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix.

6.8 : Asymmetric Key Cryptography

Q.30 What are the essential ingredients of asymmetric cipher ?

Ans. : A public key encryption scheme has six ingredients. Fig. Q.30.1 shows public key cryptography. (See Fig. Q.30.1 on next page)

1. **Plaintext :** It is input to algorithm and in a readable message or data.
2. **Encryption algorithm :** It performs various transformations on the plaintext.
3. **Public and private keys :** One key is used for encryption and other is used for decryption.
4. **Ciphertext :** This is the scrambled message produced as output. It depends on the plaintext and the key.
5. **Decryption algorithm :** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

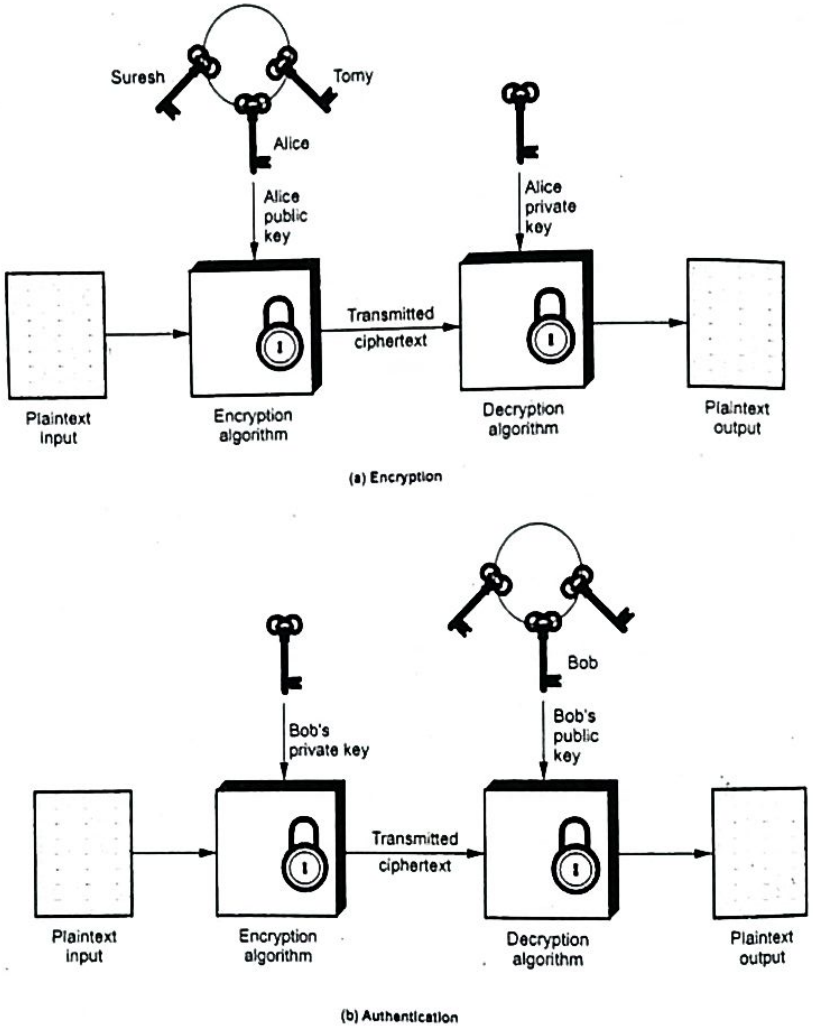


Fig. Q.30.1 Public key cryptography

- The essential steps are the following :
  1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
  2. Each user places one of the two keys in a public register. This is the public key. The companion key is kept private.

3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. Alice decrypts the message using her private key.

Q.31 Explain requirement of public key cryptography.

Ans. : Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

Q.32 Explain advantages and disadvantages of public key cryptography.

Ans. : • Advantages of public key algorithm

1. Only the private key must be kept secret.
2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
3. A private/public key pair remains unchanged for considerable long periods of time.
4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

- **Disadvantages of public key algorithm**
  1. Slower throughput rates than the best known symmetric-key schemes.
  2. Large key size.
  3. No asymmetric-key scheme has been proven to be secure.
  4. Lack of extensive history.

Q.33 Compare between symmetric key encryption and asymmetric key encryption.

Ans. :

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast	Slower
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Q.34 Explain the operation of RSA public key encryption algorithm.

Ans. : • Public key cryptography means one key is used for encryption and other key for decryption. The public key is accessed to all participants and private key is generated locally by each participant.

- RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n. RSA algorithm is public key encryption type algorithm. In this algorithm, one user uses a public key and other user uses a secret (private key) key. In the RSA algorithm each station independently and randomly chooses two large primes p

and q number and multiplies them to produce $n = p \times q$ which is the modulus used in the arithmetic calculations of the algorithm.

Key generation :

1) Pick two large prime numbers p and q, $p \neq q$;
2) Calculate $n = p \times q$;
3) Calculate $\phi(n) = (p - 1)(q - 1)$;
4) Pick e, so that gcd $(e, \phi(n)) = 1$, $1 < e < \phi(n)$;
5) Calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e. d is the multiplicative inverse of e in mod $\phi(n)$;
6) Get public key as $K_U = \{e, n\}$;
7) Get private key as $K_R = \{d, n\}$.

Encryption : For plaintext block $P < n$, its ciphertext $C = P^e \bmod n$.

Decryption : For ciphertext block C, its plaintext is $P = C^d \bmod n$.

The modulus n must be selected in such a manner that the following is guaranteed :

$$(M^e)^d) \equiv M^{ed} \equiv M \pmod n$$

- We want this guarantee because $C = M^e \bmod m$ is the encrypted form of the message integer M and decryption is carried out by $C^d \bmod n$.
- We also need to ensure that n is not factorizable by one of the modern integer factorization algorithms.
- As we have seen from the RSA design, RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to $\phi(n)$, has exponential inverse in mod n.
- Its exponential inverse d can be calculated as the multiplicative inverse of e in mod $\phi(n)$. The reason is illustrated as follows :

  Based on Euler's theorem, for y which satisfies $y \bmod \phi(n) = 1$, the following equation holds :

  $x^y \bmod n = x \bmod n$

  As $d \cdot e \bmod \phi(n) = 1$, we have that $p^{ed} \equiv P \bmod n$. So the correctness of RSA cryptosystem is shown as follows :

Encyption : $C = P^e \bmod n$;

Decryption : $P = C^d \bmod n = (P^e)^d \bmod n = P^{ed} \bmod n = P \bmod n = P$.

Q.35 List advantages and disadvantages of RSA.

Ans. : Advantages :

1. RSA can be used both for encryption as well as for digital signatures.
2. Trapdoor in RSA is in knowing value of n but not knowing the primes that are factors of n.

Disadvantages :

1. If any one of p, q, m, d is known then the other values can be calculated. So secrecy is important.
2. To protect the encryption the minimum number of bits in n should be 2048.

Q.36 List out the ingredients of public key encryption scheme.

Ans. : Ingredients of public key encryptions are :

a) Plaintext b) Encryption algorithm

c) Public key d) Private key

e) Cipher-text f) Decryption algorithm

Q.37 Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 2.

Ans. : P = 17 q = 31 and e = 7

$$n = p \times q = 17 \times 31 = 527$$

$$\phi(n) = (p-1)(q-1)$$

$$= (17-1)(31-1) = 480$$

$$d = (1 + k\,\phi(n)) / e = (1 + 480k) / 7$$

$$= -959 / 7 = -137 \quad (\text{for } k = -2)$$

$$d = -137 \pmod{480} = 343$$

Encryption $(C) = M^e \pmod n = 2^7 \pmod{527} = 128$

Decryption $M = C^d \pmod n = 128^{343} \pmod{527} = 2$

Q.38 Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.

Ans. : RSA algorithm :

$$N = p \times q = 7 \times 11 = 77$$

Calculate $\phi(n) = (p-1)(q-1)$

$$= (7-1)(11-1) = 6 \times 10 = 60$$

So, $e = 17$

Determine d such that

$$ed = 1 \bmod \phi(n)$$

$$17d = 1 \bmod 60$$

According to GCD :

$$60 = 17 * 3 + 9$$

$$17 = 9 * 1 + 8$$

$$9 = 8 * 1 + 1$$

$$8 = 1 * 8 + 0$$

Therefore, we have :

$$1 = 9 - 8$$

$$= 9 - (17 - 9) = 9 - (17 - (60 - 17 * 3))$$

$$= 60 - 17 * 3 - (17 - 60 + 17 * 3)$$

$$= 60 - 17 * 3 + 60 - 17 * 4$$

$$= 60 * 2 - 17 * 7$$

Hence, we get,

$$d = e^{-1} \bmod f(n)$$

$$= e^{-1} \bmod 60 = -7 \bmod 60$$

$$= (53 - 60) \bmod 60 = 53$$

So, the public key is {17, 77} and the private key is {53, 77}

Encryption :

Ciphertext $(C) = M^e \bmod N = (8)^{17} \bmod 77$

$$C = 57$$

6.9 : Security in Network, Transport and Application

Q.39 Give overview of IP Security. Explain applications of IPSec.

Ans. : • Different application specific security mechanisms are developed such as electronic mail (PAG, S/MIME), client/server (Kerberos), web access (secure sockets layer). An IP level security can ensure secure networking not only for applications with security mechanisms but also for many security ignorant applications.

- IP Security (IPSec) is the capability that can be added to present versions of Internet Protocol (IPv4 and IPv6) by means of additional headers for secure communication across LAN, WAN and Internet.
- IPSec is a set of protocols and mechanism that provide confidentiality, authentication, massage integrity and replay detection at IP layer. The device (firewall or gateway) on which the IPSec mechanism reside is called as **security gateway**.
- IPSec has two modes of operation.

1. Transport mode 2. Tunnel mode

- IPSec uses two protocols for message security.

1. Authentication Header (AH) protocol.
2. Encapsulating Security Payload (ESP) protocol.

Applications of IPSec

1. Secure connectivity over the Internet.

- A Virtual Private Network (VPN) can be established over the Internet. This reduces cost of private networks and network management overheads.

2. Secure remote access over the Internet.

- With IPSec, Secure access to a company network is possible.

3. Extranet and Intranet connectivity.

- With IPSec, secure communication with other organizations, ensures authentication and confidentiality and provide a key exchange mechanism.

4. Enhanced electronic-commerce security.

- Use of IPSec enhances the security in electronic commerce applications.

Q.40 Explain transport and tunnel mode of IPSec.

Ans. : Transport Mode :

- AH and ESP can support two modes of operation :
  1. Transport mode 2. Tunnel mode.
- Transport mode mainly provide protection for upper layer protocols. The protection extends to the payload of an IP packet. For example, TCP or UDP segment or ICMP packet.
- The transport mode is suitable for end-to-end communication between two workstations.
- In transport mode, ESP encrypts the IP payload excluding IP header. authentication of IP payload and specific portions of IP header.

Tunnel Mode :

- Tunnel mode provides protection to entire IP packets. Security fields are added to IP packets and entire packet (AH or ESP packet + Security packet) is new IP packet with a new IP header.
- Entire new IP packet travels through a tunnel from one point to other over IP network. No router over the network are able to detect inner IP header. Since original packet is encapsulated by new larger packet having different source and destination address.
- Tunnel mode is preferred when one or both ends of an SA a security gateway such as a firewall or router that implements IPSec.
- In tunnel mode, number of hosts on network with firewalls may engage in secure transmission without IPSec. The unsecurred packets generated are tunneled through external networks by tunnel mode SAs or IPSec in firewall or router.
- ESP encrypts and optionally authenticates the entire inner IP packet including IP header.
- AH authenticates the entire inner IP packet and selected portion of outer IP header.

6.10 : SSL

Q.41 What is SSL? List its feature.

Ans. : • SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

- SSL is designed to make use of TCP to provide a reliable end to end secure service.
- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

Features of SSL

1. SSL server authentication, allowing a user to confirm a server's identity.
2. SSL client authentication, allowing a server to confirm a user's identity.
3. An encrypted SSL session, in which all information sent between browser and server is encrypted by a sending software and decrypted by the receiving software.
4. SSL supports multiple cryptographic algorithms.

Q.42 Compare IPSec and SSL.

Ans. :

Sr. No.	Parameters	IPSec	SSL
1.	Position in the OSI model	Internet Layer	Between transport and application layers
2.	Configuration	Complex	Simple
3.	NAT	Problematic	No Problem
4.	Software Location	Kernel Area	User Area
5.	Firewall	Not Friendly	Friendly
6.	Installation	Vender Non-specific	Vender Specific
7.	Interoperability	Yes	No
8.	Deploy	More expensive to deploy, support and maintain.	Less costly to deploy and maintain

Q.43 Explain SSL handshake protocol.

Ans. : • Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption before transmitting application data various massages are used in protocol. Table Q.43.1 enlist these messages and there associated function.

Phase	Message type	Function
1.	Hello - request	Null
	Client - hello	Version, session id, cipher, compression
	Server - hellow	Version, session id, cipher, compression.
2.	Certificate	Chain of X.509 V3 certificates.
	Server - key - exchange	Parameters, signature.
	Certificate - request	Type, authorities.
	Server - done	Null
3.	Certificate - verify	Signature
4.	Client - key - exchange finished.	Parameters, signature hash value.

Table Q.43.1 SSL handshake protocol message types

- Fig. Q.43.1 shows handshake protocol action. (Refer Fig. Q.43.1 on next page)

6.11 : HTTPS and S/MIME

Q.44 Write short note on HTTPS.

Ans. : Secure HTTP is an extension to the Hypertext Transfer Protocol (HTTP) that allows the secure exchange of files on the World Wide Web.

- In HTTP basic authentication, the client sends his username and password in clear text as part of the HTTP request.
- In all subsequent HTTP requests for content from subdirectories of the original request, these credentials will be automatically resent.

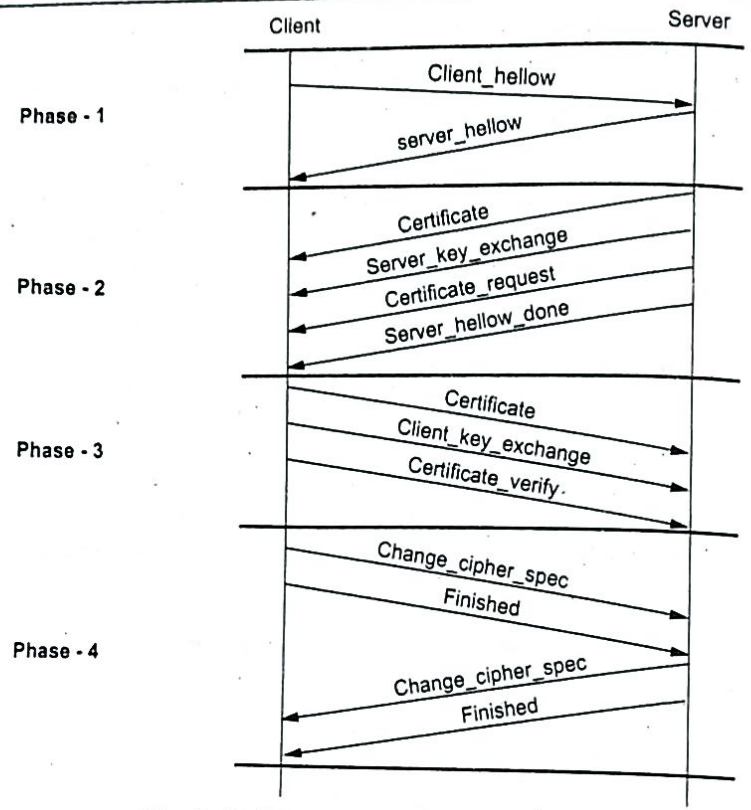


Fig. Q.43.1 Handshake protocol action

- In HTTP digest authentication, no passwords are sent in the clear. Instead, a cryptographic hash value containing the username, password and additional security-relevant data, will be transmitted from the client to the server.

HTTP Problems :

1. HTTP basic authentication is vulnerable to passive easvsdropping. Moreover, it provides no mechanism for explicit session expiration (i.e. logout).
2. HTTP digest authentication cannot guarantee sufficient support on all client platforms.
3. Both mechanisms do not provide session tracking but only authentication.

- Secure HTTP indicates to user that page contents were not viewed or modified by a network attacker.
- Each S-HTTP file is either encrypted, contains a digital certificate or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL).
- A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated. S-HTTP is more likely to be used in situations where the server represents a bank and requires authentication from the user that is more secure than a user-id and password.
- Fig. Q.44.1 shows position of HTTPS.

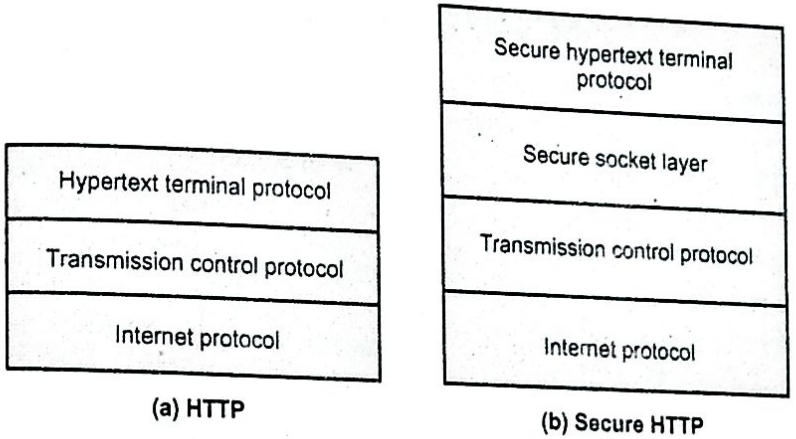


Fig. Q.44.1 Position of secure HTTP

- Secure HTTP layer is above the SSL and TCP protocol. HTTPS communicates over port 443 by default.
- Fig. Q.44.2 shows secure HTTP transactions.
- When a client makes a request over HTTPS, it first tries to locate a certificate on the server. If the cert is found, it attempts to verify it against its known list of Certificate Authorities (CA). If it is not one of the listed CAs, it might show a dialog to the user warning about the

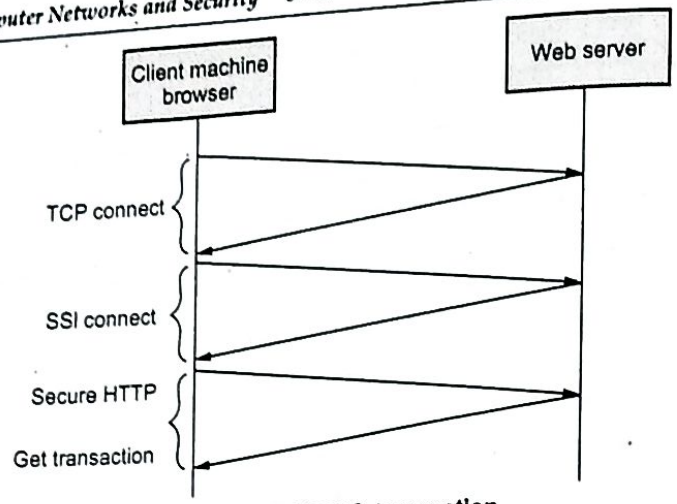


Fig. Q.44.2 HTTPS transaction

website's certificate. Once the certificate is verified, the SSL handshake is complete and secure transmission is in effect.

Q.45 What is S/MIME ? Explain functions of S/MIME.

Ans. : • S/MIME is a Secure / Multipurpose Internet Mail Extension. It is a security enhancement to the MIME Internet e-mail format standard.

- RFC 822 defines a format for text messages that are sent using electronic mail. The RFC 822 standard applies only to the contents.
- MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP.
- **SMTP limitations :**
  1. SMTP cannot transmit executable files or binary objects.
  2. SMTP cannot transmit text data that includes national language characters.
  3. SMTP servers may reject mail message over a certain size.
  4. SMTP gateways to X.400 electronic mail networks cannot handle nontextual data included in X.400 messages.
  5. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.

Function of S/MIME :

- **Functions** are as follows :
  1. Enveloped data
  2. Signed data
  3. Clear signed data
  4. Signed and enveloped data.
- **Enveloped data** consists of encrypted content of any type and encrypted content encryption key for one or more recipients.
- A **singed data** message can only be viewed by a recipient with S/MIME capability. Base64 encoding method is used for encoding content and signature.
- In **clear signed data,** a digital signature of the content is formed. Here only the digital signature is encoded using base64. Recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- **Signed and enveloped data :** Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

6.12 : Overview of IDS and Firewalls

Q.46 What is IDS ? Explain functions of IDS.

Ans. : • Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.

- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Functions of intrusion detection systems :

1. Monitoring and analysis of user and system activity.
2. Auditing of system configurations and vulnerabilities.
3. Assessing the integrity of critical system and data files.

4. Recognition of activity patterns reflecting known attacks.
5. Statistical analysis for abnormal activity patterns.

Q.47 Explain three classes of intruders.

Ans. : Three classes of intruders are Masquerader, Misfeasor and Clandestine user.

1. **Masquerader :** An unauthorized user who penetrates a computer system's access control and gains access to user accounts.
2. **Misfeasor :** A legitimate user who accesses resource he is not authorized to access. Who is authorized such access but misuses his privileges.
3. **Clandestine user :** A user who seizes the supervisory control of the systems and uses it to evade auditing and access control.

Q.48 Explain host based IDS. List its advantages and disadvantages.

Ans. : Host-based :

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails and system logs.

Advantages :

1. With their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
2. It can often operate in an environment in which network traffic is encrypted.

3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages :

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.

Q49 What is firewall ? Explain capabilities and limitation of firewall.

Ans. : • A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.

- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. Q.49.1.
- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications.

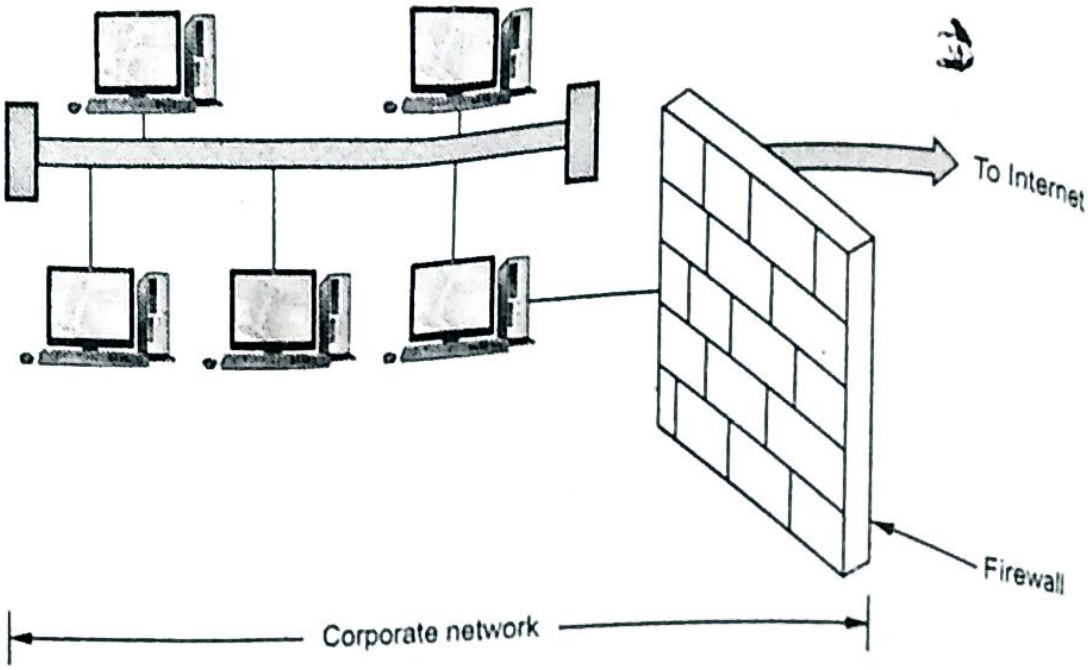


Fig. Q.49.1 Firewall

It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.

- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as **address filtering**.
- Firewalls can also filter specific types of network called **protocol filtering** because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP,FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state.

Limitations of firewall

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

END...