Maulana Bhashani Science and Technology University
Department of ICT

Name: Jannatul Ferdush Dhina

ID: IT-18012

1. a) What is network layer? Point out the functionalities of layer 3. (1+4)

b) Describe the features of network layer (4)

c) What are the services provided by layer 3? (5)

2. a) What are the types of network address? Define it. (1+4)

b) What are the Unicast routing protocols? (4)

c. Which are the Multicast routing protocols (5)

3.a) Differentiate between unicast routing and multicast routing protocols? (5)

b) Which are the characteristic and advantages of flooding algorithm? (3+3)

c) What do you know about shortest path algorithm in network routing? (3)

4. a) What is Packet Fragementation? (3)

b) What do you mean by internet protocol version 4? (5)

c) Can you elaborate Internet protocol version 6? (6)

5. a) What do you mean by transport layer? (3)

b) Define the transport layer function. (5)

c. Why transport layer services are called end-to-end? Elaborate it?

6. a) What do you mean by TCP? Elaborate it? (4)

b) What are the services of TCP? (6)

c) Define multiplexing and headers in TCP. (5)

7. a) What is UDP? (3)

b) What are the features of UDP? (5)

c) Describe about the application of UDP? (6)

8. a) Differentiate between TCP and UDP ? (6)

b) What are some real-time applications where we use TCP and UDP ? (5)

c) How does TCP/IP works ? (3)

Answer to the question no 1 (a)

Q. What are network layer ? Point out the functionalities of layer 3.

Answer: The network layer is the third layer of OSI model. It handles the service request from the transport layer and further forwards the service request to the data link layer.

The main functions performed by the network layer are:

- Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example,

5

a packet from S1 to R1 must be forwarded to the next router on the path to S2.

- Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- Internetworking: This is the main role of the network layer that it provides the logical connection between different types of network.
- Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Answer to the question no 1(b)

Q. Describe the features of network layer.

Answer: With its standard functionalities, layer 3 can provide various features as;

Quality of service management.
Load balancing and link management.
Security.
Interrelation of different protocols and subnets with different schema.
Different logical network design over the physical network design.
L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Answer to the question no-1(c)

Q. What are the services provided by layer3?

Answer: Services provided by the Network layer.

- Guaranteed delivery: This layer provides the service which guarantees that the packet will arrive at it's destination.
- Guaranteed delivery with bounded delay: This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- In-Order packets: This service ensures that, the packet arrives at the destination in the order in which they are sent.
- Guaranteed max jitter: This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- Security services: This network layer provides security by using a session key between the source and destination host. The network layer is the source host encrypts the payloads

of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Answer to the question no 2 (a)

Q. What are the types of network address? Define it.

Answer:- There are four types of network address. They are:

1. Unicast address: Unicast addresses represent a single LAN interface. A unicast frame will be sent to a specific device, not to a group of devices on the LAN.

2. Multicast Address: Multicast addresses represent a group of devices in a LAN

A frame sent to a multicast address will be forwarded to a group of devices on the LAN.

3. Broadcast address: Broddcast addressen represent all devices on the LAN. Frames sent to a broadcast address will be delivered to all devices on the LAN. The broadcast address has the value of FFFF.FFFF.FFFF (all binary ones). The switch will flood broadcast frames out all ports except the port that it was received on.

4. Anycast Routing: Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received,

it is sent to the host which is nearest in routing topology.

Answer to the question no 2(b)

Q. What are the Unicast routing protocols?

Answer: Unicast Routing Protocols:

There are two kinds of routing protocols available to route unicast packets:

- Distance Vector Routing Protocol: Distance Vector is simple routing protocol. which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately all routers build up their network topology based on the advertisement of their peer routers. For example, Routing Information Protocol (RIP)

• Link state Routing Protocol: link state protocol is slightly complicated protocol than Distance vector. It takes into account the states of links of all the routers in a network. This technique helps routers build a common graph of the entire network. All routers then calculate their best path for routing purposes. for example, Open shortest path first (OSPF) and Intermediate System to Intermediate system (ISIS).

Answer to the question no 2 (c)

Q. What are the Multicast routing protocols?

Answer: Multicast Routing Protocols: Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e spanning tree to avoid loops.

The optimal tree is called shortest path spanning tree.

- DVMRP - Distance Vector Multicast Routing Protocol.
- MOSPF - Multicast Open shortest Path First.
- CBT - Core Based Tree
- PIM - Protocol independent Multicast

Protocol Independent Multicast is commonly used now. It has two flavors:

- PIM Dense Mode - This mode uses source-based trees. It is used in dense environment such as LAN.
- PIM Sparse Mode - This mode uses shared trees. It is used in sparse environment such as WAN.

Answer to the question no 3 (a)

Q. Differentiate between unicast routing and multicast routing protocols ?

Answer: A unicast transmission/stream sends IP packets to a single recipient on a network. A Multicast transmission sends IP packets to a group of hosts on a network. If the streaming video is to be distributed to a single destination then you would start a Unicast stream by setting the destination IP address and port on the AVN equal to the destination's value. If you want to ~~w~~ view the stream at multiple concurrent locations, then you would set the AVN's destination IP address to a valid Multicast IP address (224.0.0.0 - 239.255.255.255)

Note that, While the Multicast IP address range is from 224.0.0.0 - 239.255.255.255

the first octet (224.xxx.xxx.xxx) is genarally reserved for administration. VSI recommends setting the first octet to 255 and the remaining three octets to the AVN'S IP address. for example, if the AVN'S IP address is 192.168.1.53, then set the destination IP address to 255.168.1.53 for Multicast streaming. Since Multicasting is a relatively new technology, some legacy devices that are part of your network might not support Multicasting. Before using the AVN encoder, in multicast streaming mode, check the fenctional specifications of your network infrastructure to ensure that the Multicast stream will not create major traffic on your network. Verify that, your backbone switch supports Internet group Messaging protocol (IGMP) spoo snooping, which allows the

core of your network to ignore the traffic streams that Multicasting may generate.

Answer to the question no 3(b)

Q. Which are the characteristics and advantage of flooding algorithm?

Answer: characteristics –

- All possible routes between Source and Destinations is tried. A packet will always get through if path exist.
- As all routes are tried, there will be atleast one route which is the shortest.
- All nodes directly or indirectly connected are visited.

Advantages of flooding:

- Highly Robust, emergency or immediate messages can be sent.

- Set up route in virtual circuit.
- Flooding always chooses the shortest path.
- Broadcast messages to all the nodes.

Answer to the question no 3(c)

Q. What do you know about shortest path algorithm in network routing?

Answer: Data transfer operations is a crucial aspect in case of networking and routing. So, efficient data transfer operations is a must need, with minimum hardware cost and also in the minimum time possible. Thus, the need is to propose an algorithm that finds the shortest path between two nodes (source node and destination node)

Let's see a completely new algorithm unlike Dijkstra shortest path or any

other algotrithm for finding shortest path.

Answer to the question no 4(a)

Q. What is Packet Fragmentation ?

Answer: Packet fragmentation can be handle at many different protocol layers. TCP already includes packet reassembly. If your dissector needs to do additional packet reassembly then you can utilize the reassembly functions defined in Ethereal. A good example of how to handle packet reassembly by TCP is located in section 2.7 of the README. Developer document in the doc directory. It covers how to handle the packet reassembly when your dissector is running on top of TCP or User Datagram Protocol (UDP). The files packet-tcp2222.inc, packet-atalk.c, and packet-clnp.c all give examp

of how to defragment messages that are fragmented within the protocol you are dissecting. The logic involved in defragmented packets can be very complicated. You will find yourself spending many hours troubleshooting and fine-tuning the defragmentation function.

Answer to the question no 4 (b)

Q. What do you mean by internet protocol version 4 ?

Answer: Internet Protocol Version 4 (IPv 4) is the fourth revision of the internet protocol and a widely used protocol in data communication over different kinds of network. IPv4 is a connectionless protocol used in packet-switched layer networks, such as

Ethernet. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices - including manual and automatic configurations - depending on the network type. IPv4 is based on the best-effort model. This model guarantees neither delivery nor avoidance of duplicate delivery, these aspects are handled by the upper layer transport. IPv4 is defined and specified in IETF publication RFC 791. It is used in the packet-switched link layer in the OSI model. IPv4 uses 32-bit addresses for Ethernet communication in five

classes: A, B, C, D and E. Classes A, B and C have different bit length for addressing the network host. Class D addresses are reserved for multicasting, while class E addresses are reserved for future use.

Class A has subnet mask 255.0.0.0 or /8, B has subnet mask 255.255.0.0 or /16 and class C has subnet mask 255.255.255.0 or /24. For example, with a /16 subnet mask, the network 192.168.0.0 may use the address range of 192.168.0.0 to 192.168.255.255. Network hosts can take any address from this range, however address 192.168.255.255 is reserved for broadcast within the network. The maximum

number of host addressed IPv4 can assign end to users in 232. IPv6 presents a standardized solution to overcome IPv4's lamination. Because of it's 128-bit address length, it can define upto 2,128 address.

Answer to the question no 4(e)

Q. Can you elaborate internet protocol version 6?

Answer: IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv6 exhustion. IPV6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation.

There was 8 groups and each group represents 2 Bytes.

In IPv6 representation, we have three addressing methods:

- Unicast
- Multicast
- Broadcast

Unicast Address: Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.

Mutticast Address: is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interface corresponding to that multicast address.

Anycast Address: Anycast Address is assigned to

a group of interface. Any packet sent to Any-cast address will be delivered to any one number interface (mostly nearest host possible).

Answer to the question no 5 (a)

Q. What do you mean by transport layer?

Answer: Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer and then breaks it into smaller size segments, ~~an~~ numbers each byte. and hands over to lower layer for delivery.

Answer to the question no 5 (b)

Q. Define the transport layer functions?

Answer: This layer is the first one which breaks the information data, supplied by Application

layer in to smaller units called segments. It numbered every byte in the segment and maintains their accounting.

This layer ensures that data must be received in the same sequence in which it was sent.

This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.

All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points also known as port numbers.

Answer to the question no 6(a)

Q. What do you mean by TCP ? Elaborate it.

Answer: The transmission control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets.

i) Recognizing and reserding lost packets.

ii) Detecting and dropping duplicate packets.

iii) Recognizing and reordering the packets that arrive out of order.

iv) Controlling the overflow of segments.

Answer to the question no-6(b)

Q. What are the services of TCP ?

Answer: The Transmission Control Protocol is the most common transport layer protocol. It work together with IP and provides a reliable transport service between processes using

the network layer service provided by the IP protocol.

The various services provided by the TCP to the application layer are as follows:

1. Process to process communication -
This provides process to process communication i.e the transfer of data takes place between individual process executing on end systems.

2. stream oriented -
This means that, the data is sent and received as a stream of bytes However, the network layer, that provides service for the TCP, sends packets of information not stream of bytes.

3. Full duplex service -
This means that the communication can take place in both directions at the same time.

4. Connection oriented service -
Unlike UDP, TCP provides connection oriented service. It defines 3 different phases.

- Connection establishment
- Data transfer
- Connection termination

5. Reliability - TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgement policy and timers.

6. Multiplexing - TCP is reliable as it uses checksum to. does multiplexing and de-multiplexing at the sender and receiver ends respectively as a number of logical connections can be established between port numbers over a physical connection.

Answer to the question no – 6 (c)

Q. Define Multiplexing and headers in TCP.?

Answer: A TCP connection is specified by a 4-tuple (source IP address, source port, destination IP address, destination port)

- TCP allows multiplexing of multiple connection between end systems to support multiple applications simultaneously.
- Arriving segment directed according to connection 4-tuple.

TCP Header:-

Port Numbers –

- A socket identifies a connection endpoint -IP address + port
- A connection specified by a socket pair.
- Well known ports –
  - FTP 20
  - Telnet 23
  - DNS 53

- HTTP 80

Sequence Number

- Byte count
- First byte in segment
- 32 bits long
- $0 \leq SN \leq 2^{32}-1$
- Initial sequence number selected during

Connection setup.

Answer to the question no 7 (a)

Q. What is UDP ?

Answer: User Datagram Protocol (UDP) is a Transport layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is th

dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services, like computer gamming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP so it also saves bandwidth.

Answer to the question no 7 (b)

8. What are the features of UDP?

Answer: Features of UDP,

- Provides connectionless, unreliable service.
- So UDP faster than TCP.

- Adds only checksum and process-to-process addressing to IP.
- Used for DNS and NFS.
- It Used when socket is opened in datagram mode.
- It sends bulk quantity of packets.
- No acknowledgment.
- Good for video, streaming it is a unreliable protocol.
- It does not care about the delivery of the packets or the sequence of delivery.
- No flow control/congestion control, sender can overrun receiver's buffer.
- Real time application like video conferencing needs.

Answer to the question no - 7 (c)

Q. Describe about the application of UDP ?

Answer: Applications of UDP:

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- It is suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP (Routing Information Protocol)
- Normally used for all real time applications which cannot tolerate uneven delays between sections of a received message?
- Following implementations uses UDP as a transport layer protocol.
  - NTP (Network Time Protocol)
  - DNS (Domain Name service)
  - BOOTP, DHCP
  - NNP (Network News Protocol)

- Quote of the day protocol
- TFTP, RTSP, RIP, OSPF.
- Application layer can do some of the tasks through UDP-
  - Trace Route
  - Record Route
  - Time stamp
- UDP takes datagram from Network layer, attach its header and send it to the user. So, it works fast.
- Actually UDP is null protocol if you remove checksum field.

Answer to the question no 8(a)

Q. Differentiate between TCP and UDP?

Answer:

TCP	UDP
It is a connection orcienred protocol.	It is a connectionless protocol.

TCP	UDP
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed of TCP is slower	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	Header size is 8 bytes.
TCP is reliable as it guarantees delivery of data to the destination routers.	The delivery of data to the destination can't be guaranteed in UDP.

Answere to the question no - 8 (b)

Q. What are some real-time application where we use TCP and UDP?

Answer: UDP:

- Tunneling/VPN (lost packet are ok - the tunneled protocol takes care of it)
- Media streaming (lost frames are ok)
- Games that don't care if you get every update
- local broadcast mechanisms (same application running on different machines "discovering" each other)

TCP:

- Web
- SSH, FTP, telnet
- SMTP, sending mail
- IMAP/POP, receiving mail.

Answer to the question no 8 (c)

Q. How does TCP/IP works?

Answer: TCP allows for transmission of information in both direction. This means that, computer systems that communicate over TCP can send and receive data at the same times, similar to a telephone conversation. The protocol uses segments (packets) as the basic units of data transmission. In addition to the payload, segments can also contain control information and are limited to 1,500 bytes. The TCP software in the network protocol stack of the operating system is responsible for establishing and terminating the end to end connections as well as transferring data.

The TCP software is controlled by the various network applications, such as, web browsers or servers, via specific interfaces. Each connection must always be identified by two clearly defined endpoints. It doesn't matter which side assumes the client role and which assumes the server role. All that matters is assumes the client role and which that, the TCP software is provided with a unique, ordered pair consisting of IP address and port for each endpoint.