

1

CT-02

New
questions

Name: Zafraul Hasan Khan ID:- IT-18003

1. (a). what is the function of data link layer?

- (b) which address is used in data link layer?
What is link layer design issue? 3+2

(c) which is most efficient error detection and correction method? why do you need error detection? 2+3

2. (a). what are the flow control protocols? 3

- (b) what is the responsibility of data link layer? which device is used in data link layer? 2+3

(c) why flow control and error control

6

2

mechanism are implemented in data link layer as well as transport layers?

Q. 3.

(a). Which is the main function of network layers?

5

(b) IS IP a network layer? 3

(c) What are the features of a network layer protocol? Explain.

6

4. (a). Is a network address an IP address? 4

(b) Why is networking addressing

4

important? 4

(c) What is classful addressing in networks? Why is it important to have a unique IP? 2+4

2+4

3

5(a). What is routing in network layers? 2

(b) which routing protocols use multicast?

What devices uses multicast? Does multicast

work over wifi? 2+2+2

(c). What is anycast and how does it

works? How do you implement anycast?

2+4

6(a). what is unicast and multicast

protocols? How do you ping

2+2

multicast address?

(b) How can you if your network is

flooded? What routing technique is

2+3

(c) which algorithm is used to find all

pairs shortest path? What is the

2+3

shortest algorithm?

4

- Project 7.
- (a) what is the purpose of internet working? what is an internet system? what is a working device? 3+2
- (b). How is tunneling done? how does it work on a VPN? 2+2
- (c). What causes packet fragmentation? How do you prevent packet fragmentation? 3+2
8. (a). How does address resolution work? 3
- (b). Which utility uses the internet control messaging protocol? what are the two forms of ICMP? what is the relationship between IP and ICMP? 2+3
- (c) what is the difference between IPv4 and IPv6? 6

1.(a) What is function of data link layer?

Ans. The data link layer takes the data bits and frames and creates packets of the data frame to guarantee reliable transmission.

This layer adds source and destination addresses to the data stream as well as information to detect and control transmission errors.

Data link layer does many tasks on behalf of upper layer such as:

- Framing: Data link layer takes packets

from network layer and encapsulates them into frames.

to groups of QLLM20 do now

• Synchronization: When data frames sent on the link, both machines must be synchronized in order to transfer to take place.

6

• Error control: Sometimes signals may have encountered problems in transition to bits and these bits are flipped. These errors are detected and attempted to recover the actual data bits.

• flow control: stations on some link may have different speed or capacity.

Data link layer controls are used to ensure no error from both machine to exchange data on same speed.

Besides, data link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems.

7

Q. (b) Which address is used in data link layer? What is data link layer design issue?

Ans: The source and destination of MAC addresses are used in the Data-Link frame header for protocols that use MAC addresses. IP (both IPv4 and IPv6) uses network layer addresses that are used in the network layer packet header.

Data link layer design issue: The data link layer in the open system interconnect (OSI) model is between the physical layer and the network layer. This layer converts the raw transmission facility provided or by reliable and error-free link.

Q. 1(c) which is the most efficient error detection and correction method? Why SAM do not need error detection?

Data sent in binary form is error-free.

Ans: The best known error-detection method is called parity, where a

single extra bit is added to each byte of data and assigned a value

of 1 or 0, typically according to whether

there is an even or odd number of bits needed for detection.

Whenever a message is transmitted, it may

get scrambled by noise or data may

get corrupted. To avoid this, we

use to encode - detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission according to the message.

Besides many communication channels are subject to channel noise and thus errors may be introduced during transmission from the source to receiver. Error detection techniques allow detecting such errors,

while error detection and correction enables reconstruction of the original data in many cases. Previous work, studies of what happened after errors, transmission, revision, etc. of

Q. What does the flow control protocols?

Ans: Flow of controls in computer networks

is a set of procedures to restrict

the amount of data that sender

can send. Stop and wait protocol

is a flow control protocol where

sender sends one data packet to the

receiver and then stops and waits

for its acknowledgement from the

receiver. In hosts, sliding window

receives and processes the data

packet. receiver sends an acknowledgement

to the sender. After receiving the

acknowledgement, sender send the next data

packet to the receiver.

Q. (b): What is the responsibility of data link layer? Which device is used in data link layer?

Ans: The data link layer is responsible for multiplexing data streams, data frame

detection, medium access and error control.

It ensures reliable point to point and point to multipoint connections in a communication network.

Data link layer uses in devices: Two types of Data Link layer devices are commonly used on networks: bridges and switches.

A bridge is an intelligent repeater that is aware of the MAC addresses of the nodes on either sides of the bridge.

12

2. (c). Why flow control and error control mechanism are implemented

in data link layer as well as

transport layer?

Ans: Flow control in transport layer ensures the timely delivery of the message

globally, i.e. as there are two points of

connection over this protocol are physically connected.

Actually in transport layers two points connection are

logically connected.

Whereas in data-link layer, the concern is to deliver message locally.

about the two points of connection

over this protocol are physically connected.

Now, coming upon the algorithms that controls flow of a network.

Stop and wait: This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data frame sent is received.

Sliding window: In this flow control mechanism, both sender and receiver agree on the number of data frames after which the acknowledgement should be sent.

That's why error control and flow control are implemented in data link layer and transport layer.

between which is the main function of network layers?

~~host to host~~ 2007-08

Ans: The main function of the network layer is to move the packets from

host to host to the receiving host.

~~host to host~~ 2007-08

The main function performed by the network layers:

- **Routing:** When a packet reaches the router's input link, the router will

move the packets to the router's output link.

- **Logical Addressing:** The data links

implements the physical addressing

and network layer implements the

15

Logical addressing.

• 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.

3. (b) Is IP network layer?

Ans: IP is connectionless, that is a data packet can travel from sender to a recipient without the acknowledgement.

orientated protocols exist at others, higher

16

layers of OSI model. The TCP/IP

internet layers are equated with the

OSI network layers. The TCP/IP internet

layer is in fact only a subset

of functionality of the network

layer.

What are the features of

a network layer protocol? Explain.

Ans:

Features of network layer

Static IP routing. Every wireless

routers includes static IP routing.

static routing enables you to configure permanent IP routes.

To fix destination addressing.

~~Dynamic IP routing~~: Some wireless routers include dynamic IP routing. These routers support one or more dynamic routing protocols.

~~Dynamic host configuration~~: Protocol server:

A Dynamic host configuration protocol server allows the allocation and reuse of IP addresses as end user need them.

~~Point to Point Protocol over Ethernet~~:

point to point protocol over Ethernet

allows an ISP to authentic end

user some wireless router support

PPPoE by passing PPPoE packet to the

PPPoE server -

Local balancing and link management.

Interrelation of different protocols

and subnets with different scherrna. grifwors

** Different logical network design over

the physical network design.

~~next~~ security ~~new~~ ~~new~~ ~~do~~ members

~~quality~~ quality of service management.

1970-1974
1975-1979
1980-1984
1985-1989
1990-1994
1995-1999
2000-2004
2005-2009
2010-2014
2015-2019

luteo *sitrenatus*

6709902 5-1 6721 500 200110

2005 2006 2007 2008

69999 69999

00999

• १८८६२ दृष्टि

Q. (a) Is there a network address among IP addresses?

Ans: Routing network address is an IP

address without host address. In technical

term, a network address is an IP

address in which all host bits are turned off. we can only turn on or off hosts.

In other terms, to facilitate communication between multiple interconnected

networks, the IP address is broken

into parts. one part is the network

address and the other part is the local address. Each network has a

local address. Each network has a

unique network address and every device on that network has the same IP address.

Q(b) why is network addressing important?

Ans: In the world of telecommunications and networking there are millions of

computers and devices connected at numerous geographical locations communicating each other.

Similar to millions of people in a nation, there has to be means by

which people are identified as individuals and located for effective communication

to occur. Networks are formed with computers and other communication devices, IP and MAC addresses are therefore mechanisms within networks by which the devices are identified and located and for communication.

People are identified as individuals using social security numbers, for example, and their location (home / business) by physical address.

22

4(c) What is classful addressing in computer networks? Why is it important to have a unique IP?

Ans: A classful network is a network addressing architecture used in the Internet from 1981 until the introduction of classless Inter-Domain Routing in 1993.

The method divides the IP address space (IPv4) into five classes based on the leading four address bits.

Important to know have a unique IP: When you're putting up a website on the internet you'll have a lot of options when it comes to hosting. Most people don't go through the expense or the hassle of setting up their own server and have to work with their own web host. Effectively becoming their own web host. Their other options would be to use a dedicated server or shared web hosting. If your web host offers a dedicated server you will be able to have your own private IP address for your website. This makes it impossible for your website to be affected by the shenanigans.

from other webmasters. A unique IP address
provides a layer of protection and
greater security and reliability. Not
many hosts share the same IP address.

Ques. (a) What is routing in network
layer?

Two main paths to select.

Ans. Routing is the process of selecting
a path for traffic flow.

Network or between multiple
hosts.

Broadly, Routing is performed
between networks.

in many types of networks,

including circuit-switched networks, such
as the public switched telephone network.

and computer networks, such as the
internet.

Ques: Which routing protocols use multicast?

Ans: Does multicast work over wifi?

Ans: Routing protocols (RIPV2, EIGRP and OSPF) use multicast addresses to speak

to their neighbours. For example, OSPF routers use 224.0.0.6 to speak to the

designated router (DR) in a multi-access network.

multicast address range from 224.0.0.0 to 239.255.255.255.

uses broadcast traffic

multicast and broadcast are a normal part

of all networks

today, many devices

broadcast traffic to advertise and discover services on the

multicast broadcast traffic to advertise and discover services on the

network. protocols such as bonjour

and MDNS make streaming to an

Apple TV or connecting to a printer

simple but that simplicity at a cost.

multicast work over wifi: To make

multicast work over wifi successfully

we often need to modify the multicast

variables instead be sent as unicast in order

successfully transmit with

useable quality. Multicast over wifi

experiences high packet error rates, no

acknowledgements and low data rate.

No winner never

has to

of without

no winner never

brown

Q5(c). what is anycast and how does it work? How do you implement anycast?

→ ~~Sharing IP address~~: no Hosts, multiple hosts

Ans: In anycast, a collection of servers share the same IP address and send data from a source computer to the server that is topographically closest. This helps cut down on latency and bandwidth costs, improves download time for users and improves availability.

Implementation of Anycast: Anycast can be implemented on the router in two ways:

1. ~~Hosts~~ → use a static route on the first hop of router or enable e.

2. ~~Protocol~~ → on the server.

Routing protocol is used here.

the following steps will be necessary before implementing Anycast:

- + Anycast Address Selection: current practice is to assign small subnet of anycast addresses from unicast IP space.
- + Location of the server: The network will perform load balancing if servers are widely distributed with higher density in and surrounding high-demand areas.

Server and service configuration:

server need to get a second address used for Anycast.

- + Anycast testing: The Anycast testing service is ready to be tested and used when all is working properly.

Q. (4) what is unicast and multicast routing protocols? How do you ping a multicast address?

priv0017 at 6:19:10

Ans: In unicast transmission / stream sends IP packets to a single recipient on a network.

In hosts a multicast transmission sends IP packet to a group of hosts on a network.

Now, if we ping a multicast address, we can only ping,

hosts which are subscribed via multicast, to the multicast group which you are pinging. You need to be careful about

which multicast groups you use, and in general you should use multicast administratively scoped groups from the range of 239.0.

30

C.(b) How can you know if your network is flooded? What routing technique is applied in flooding?

Ans: The first step to recognizing the network flooding attack is by applying the detection system like Snort. Snort is an open source system that can be used to detect flooding attacks using special rules owned by Snort.

Routing technique in flooding: Routing is applied by the way of simplest method packet forwarding.

Flooding is a simple routing technique in computer networks.

where a source or nodes sends packets through every outgoing link. Flooding, which is similar to broadcasting, occurs when source packets (without routing data) are transmitted to all attached network nodes.

6(c). Which algorithm is used to find all pairs shortest path? What is the best shortest path algorithm?

Ans: Floyd-Warshall algorithm is used to find all pairs shortest path. The all pair shortest path algorithm is also known as Floyd-Warshall algorithm is used to find all pair shortest path

32

problem ~~is~~ given a weighted graph. As a result of this algorithm, it will generate a matrix, which will represent the minimum distance from any node to all other nodes in the graph.

Best shortest path algorithm: Dijkstra finds the shortest path from only one vertex, while Floyed-Warshall finds the shortest path between all of them.

If I want to find the shortest path between all pairs of vertices as it has a higher priority than Dijkstra algorithm.

Dijkstra algorithm runs faster than Floyed-Warshall as we can use negative weights. Dijkstra cannot be used for graphs with negative weights.

- o 2) Ques: What is the purpose of internetworking? What is an internet interworking device?
- o Ans: Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers. Routers are gateway devices. Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the internet routing protocol.
- o Internet Interworking Device: An internet interworking device is a widely used term for any hardware within networks that connect different network resources. Key device

that comprise network area routers, bridges, repeaters and gateways in networks.

Q(b). How tunnelling is done? How does tunnelling work on a VPN?

Ans: A parallel pair of walls are embedded into the ground along the tunnel's route by driving steel sheets or constructing slurry walls. A trench is dug between the walls to a depth equal to the planned distance inside out of the tunnel roof. Rollers

Tunnelling on a VPN: A VPN tunnel is an encrypted link between your computer on mobile device and an outside network. A VPN tunnel connects your smartphone, laptop, computer, tablet to your

another network in which your IP and
addresses is hidden and all the data
you generate while surfing the web
is encrypted.

Q. What causes packet fragmentation?
Ans: How do you prevent packet
fragmentation?

Ans: Fragmentation occurs when an IP
datagram traverses a network which
has a maximum transmission unit
that is smaller than the size of

the datagram. If a larger size of
datagram was to traverse an Ethernet
network it would require fragmentation

to prevent it being discarded somewhere

36.

along the path.

prevent packet fragmentation: A sender can set the don't fragmentation flag in the IP header, asking intermediate routers never to perform fragmentation of a packet. Instead a router with a link having a smaller MTU will send an ICMP message "backwards" to the sender to reduce the MTU sent to the receiver.

I20 bmo 51000100 I20 sent presented

2 21000100 99A . royal sin

privat 91 ni noitgnr beriwer

8.(a) How does address resolution protocol work?

Ans: The address resolution protocol (ARP)

is a protocol used by the internet

protocol, specially IPv4, to map IP

network addresses to the hardware

addresses used by a data link protocol.

The protocol operates below the network

layer as a part of the interface

between the network and OSI

link layer. ARP feature performs a

required function in IP routing.

Q(b) which utility uses the internet

of control messaging protocol? what are the two forms of ICMP? what is the relationship between IP and ICMP?

Ans: ping is a utility which uses ICMP

ping formats to report back information on network connectivity and the speed of data relay between a host and a destination computer.

Two form of ICMP: There are two

types of ICMP messages that are used.

such as Echo request and Echo reply.

Reply.

Relationship between IP and ICMP:

ICMP creates and sends messages to the source IP address indicating that

a gateway to the internet that a

router, service or host cannot be reached

for packet delivery.

Any IP network device has the capability to send, receive or process ICMP messages. ICMP is not a

transport protocol that sends data between systems.

Q(c). what is the difference between IPv4 and IPv6.

M2JY 215107962 PVII
M2JY forming IPmax limitiv,

IPv4	IPv6 (HARD)
IPv4 is a 32-bit IP address. of 4 octets (quadrenary).	IPv6 is a 128-bit IP address.
IPv4 is a numeric addressing method.	IPv6 is an alpha-numeric addressing method.
IPv4 binary bits are separated by a dot (.)	IPv6 binary bits are separated by a colon (:) .
IPv4 offers 12 header fields.	IPv6 offers 8 header fields
IPv4 supports broadcast.	IPv6 doesn't support broadcast.
IPv4 has checksum.	IPv6 doesn't have checksum.

41

IPv4	IPv6
IPv4 supports VLSM (Virtual Length subnet Mask)	IPv6 doesn't support VLSM.
IPv4 uses ARP (Address Resolution Protocol) to map to MAC Address	IPv6 uses NDP (Neighbour Discovery protocol) to map to link address

Robert & Webb IPv4 vs Robert & Webb IPv6

Robert & Webb IPv4 vs Robert & Webb IPv6

(: notes)

Robert & Webb IPv4 vs Robert & Webb IPv6

Ability

Ability

Robert & Webb IPv4 vs Robert & Webb IPv6

Protocol

Robert & Webb IPv4

Protocol

Protocol Client IPv4