Department of Computer Science
University of Karachi
BCS Program (6th Semester)

2342-Computer Networks
Terminal Examination Date: 16-Jan-2020
Max. Time: 2 Hours Max. Marks: 48

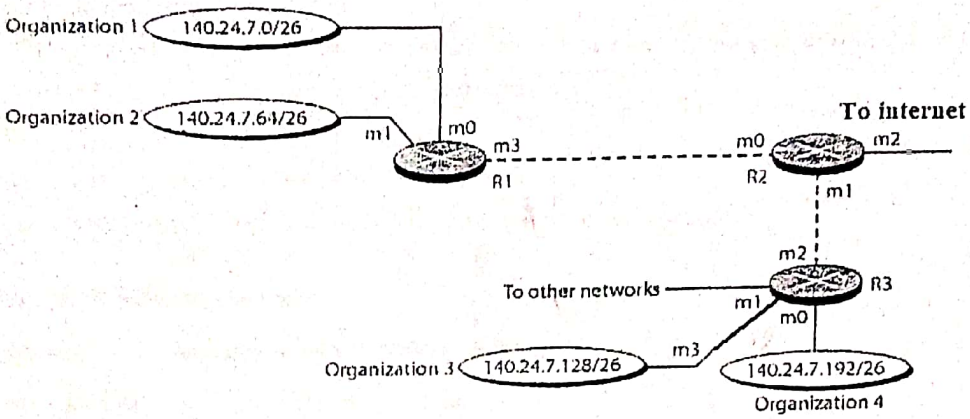
Seat Number:	Name:
Enrollment Number:	Institute/College:

Instructions:

1) *Attempt all questions. Explain the answers by elaborating the diagram where necessary.*
2) *Do not write on question paper except Name, Seat Number and Enrollment Number.*
3) *Please return the question paper along with your answer script.*

Question 1: **(12)**

a) Define the term VLAN? Explain the benefits of VLAN?
b) Differentiate between link state routing algorithm and Distance Vector Routing Algorithm?
c) Make a routing table for Router R1, R2 & R3 using the configuration given in the figure.

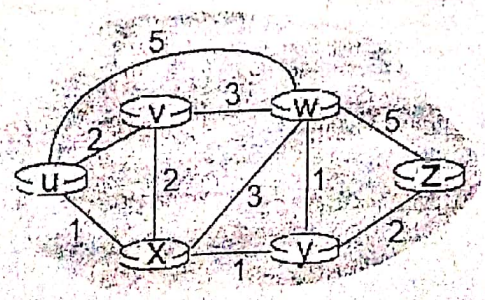


Question 2: **(12)**

a) How the QoS and security achieved in IPV6? Differentiate between switching and routing?
b) How do an IP address and its subnet mask function together?
c) Consider sending a 2400-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are generated? what are the values in the various fields in the IP datagram(s) generated related to fragmentation?

Question 3: **(12)**

a) Differentiate between TCP Vs UDP why TCP is better than UDP. Give name of two applications that are based on TCP?
b) IP protocol work on network layer? IP protocol is a connectionless protocol if you agree justify your answer or not, why not?
c) Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from u to all network nodes. Show how the algorithm works by computing a complete table.



Question 4: **(12)**

a) Define the three-way handshake for reliable connection establishment and termination that TCP used?

b) Differentiate between the following

i) NAT vs PAT
ii) access routers vs border routers
iii) Fragmentation and Segmentation

c) For the following, determine the network address & the broadcast address.

i.	15.5.16.35	255.255.255.192
ii.	212.172.38.172	255.255.128.0
iii.	108.163.212.191	255.255.224.0

Data Communication 16-Jan-2020

Q#1 (a)

Define the term VLAN? Explain the benefits of VLAN?

VLAN:

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as "Virtual Local Area Network".

Benefits of VLAN:

1- Reduction in cost

2- Saving of time required for rewiring.

3- VLAN's provide additional security. The message broadcast in one group cannot be listened by members of the other groups

4- No need to change physical configuration.

5- It solves a broadcast problem.

6- It reduces the size of broadcast domains.

7- It allows you to add an additional layer of security.

8- It can make device management simple and easier.

9- Higher performance and reduced latency.

10- It provides increased performance.

11- It remove the physical boundary.

12- It lets you easily segment your network.

13- It helps you to enhance network security.

14- You can keep host separated by VLAN

15- You do not required additional hardware and cabling which helps you to reduce cost.

Q#1(b)

Differentiate b/w link state routing algorithm and Distance vector routing algorithm?

Distance Vector	Link state
1- It is a dynamic routing algorithm in which each router computes distance b/w itself and each possible destination i.e. its immediate neighbors.	It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
2- Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwith required is more due to flooding and sending of large link state packets.
3- Make use of Bellman Ford algo.	Make use of Dijkastra's algo.
4- Traffic is less.	Traffic is more.
5- Converges slowly i.e. good news spread fast and bad news spread slowly.	Converges faster.

Distance Vector	Link state
6- Count to infinity problem.	No count to infinity problem.
7- It sends complete routing table.	It sends only link state information.
8- Updates are sent using broadcast technique.	Updates are sent using multicast technique.
9- It doesn't know the network topology.	It knows the network topology.
10- Very simple to configure.	Difficult to configure.
11- Susceptible to routing loops.	Less susceptible to routing loops.

Q#1(c)

Make a routing table for Router R1, R2 & R3 using the configuration given in the figure.

Routing Table for R1:-

Mask	Network Address	Next-hop Address	Interface
/26	140.24.7.192	--------	m3
/26	140.24.7.128	--------	m3
/26	140.24.7.64	--------	m1
/26	140.24.7.0	--------	m0
/0 (Default)	0.0.0.0	0.0.0.0	m3

1st 2nd Solved 4th 3rd

* these should be solved Decendingly

Routing Table for R2:-

Mask	Network Add	Next-hop Add	Interface
/26	140.24.7.192	-------	m1
/26	140.24.7.128	-------	m1
/26	140.24.7.64	-------	m0
/26	140.24.7.0	-------	m0
/0	0.0.0.0	0.0.0.0	m2

Routing table for R3 :-

Mask	Network Add	Next-hop Add	Interface
/26	140.24.7.192	- - - - - - -	m0
/26	140.24.7.128	- - - - - - -	m3
/26	140.24.7.64	- - - - - - -	m2
/26	140.24.7.0	- - - - - - -	m2
/0	0.0.0.0	0.0.0.0	m2

Q#2(a)

How the QoS and security achieved in IPv6? Differentiat b/w switching and routing?

Security in IPv6:

Unlike IPv4, IPsec security is mandated in the IPv6 protocol specification, allowing IPv6 packet authentication and/or payload encryption via the Extension Headers. However, IPsec is not automatically implemented, it must be configured and used with a security key exchange.

(7)

QoS (Quality of Service) in IPv6:

The IPv6 header has a structure that identifies the flow of packets (Flow Label Field) and thereby directs it to the router.

Difference b/w switching and Routing:

geeksforgeeks

Routing	Switching
1) Its function to route packets b/w different networks (b/w different LANs).	Its function to switch data packets b/w devices on the same network (or same LAN).
2) They operate at layer 3 of the OSI Model (Network layer).	They operate at layer 2 of the OSI Model (Datalink layer).
3) The main objective is to connect various networks simultaneously.	The main objective is to connect various devices simultaneously
4) Router is used by LAN as well as MAN. (Metropolitan Area Network).	Switch is used by only LAN. (Local Area Network)

* IP: Internet Protocol
* MAC: Media Access Control
* ASIC: Application Specific Integrated Circuit

Routing	Switching
5) Data is sent in the form of packet.	Data is sent in the form of packet and frame.
6) It's a full duplex mode transmission	It's also a full duplex mode transmission.
7) There is less collision take place in router.	There is no collision take place in full duplex switch
8) It is compatiable with NAT. (Network Address Translation)	It is not compatiable with NAT.
9) Routing is done by using IP address.	Switching is done by using MAC Address
10) Routing is done in different network	Switching is done in same broadcast domain.
11) Routing will be slower as it is software based	Switching will be faster as switch uses ASIC technology.

Q#2(b)

How do an IP address and its subnet mask function together?

Subnet mask divides the IP address into a network address and host address, hence to identify which part of IP address is reserved for the network and which part is available for host use. Once given the IP address and its subnet mask, the network address (subnet) of a host can be determined.

Usually, subnet calculators are readily available online that help divide an IP network into subnets.

Q#2(c)

Consider sending a 2400-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?

(10)

Given Data:

Datagram = 2400 byte (IP header = 20 + Payload (data) = 2380)

IP header = 20 byte

MTU (Maximum Transmission Unit) = 700 bytes

Identification number = 422

Total number of fragments generated = ?

Various fields values generated related to fragments = ?

Sol: Total number of fragments generated:

$$\text{Total Fragments} = \left[\frac{\text{Datagram} - \text{IP header}}{\text{MTU} - \text{IP header}}\right]$$

$$= \left[\frac{2400 - 20}{700 - 20}\right]$$

$$= \left[\frac{2380}{680}\right]$$

$$= [3.5]$$

≈ 4 (We should always consider ceil value)

Total Fragments = 4

* MF: More Fragments: It looks for next fragment (1 or 0)
* TL: Total Length : IP header + Payload
* Offset: It gets "ahead" Data $\left(\frac{\text{Payload}}{8}\right)$ | $\left(\text{To get payload} = \text{offset} \times 8\right)$

(11)

Various fields values generated related to fragments:

Fragment number	Datagram Payload (Data Part)	Identification number	Offset	MF	TL
1	680	422	0	1	700
2	680	422	85	1	700
3	680	422	170	1	700
4	340	422	255	0	360

Q#3(a)

Differentiate b/w TCP Vs UDP why TCP is better than UDP. Give name of two applications that are based on TCP?

TCP	UDP
1- It stands for "Transmission Control Protocal".	It stands for "User Datagram Protocal".
2- It is a connection-oriented protocal.	It is a connectionless protocal.
3- The speed for TCP is slower.	UDP is faster as error recovery is not attempted.

TCP	UDP
4- Header size is 20 bytes	Header size is 8 bytes
5- TCP is heavy weight.	UDP is lightweight.
6- TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
7- Acknowledgment segments.	No Acknowledgment segments.
8- TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.

TCP is better than UDP because of following reasons:

→ TCP is reliable as it provides reliability of delivery of packets to the receiver while UDP is non-reliable and does not give information about the packets.

→ TCP provides flow control and error control characteristics while UDP doesn't provide it.

Following are the two TCP based application:

1- World Wide Web (WWW)
2- Email

Q#3(b)

IP protocol work on network layer? IP protocol is a connectionless protocol if you agree justify your answer or not, why not?

IP protocol on network layer:

The IP (Internet Protocol) is a protocol that uses datagrams to communicate over a packet-switched network. The IP protocol operates at the network layer protocol of the OSI reference model and is a part of a suite of protocols known as TCP/IP.

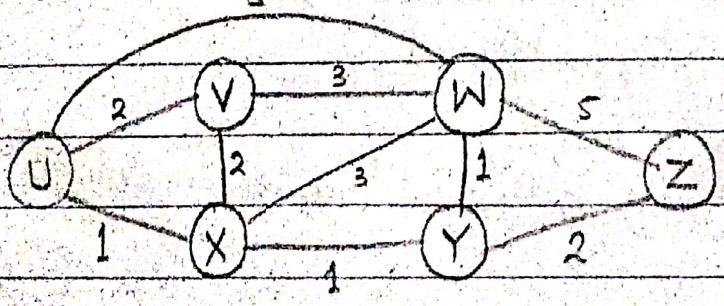
IP protocol is a connectionless protocol:

IP Protocol is a connectionless protocol ~~that~~ in which all packets in IP network are routed

independently, they may not necessarily go through the same route, while in a virtual circuit network which is connection-oriented all packets go through the same route.

#3(c)

Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from U to all network nodes. Show how the algorithm works by computing a complete table.

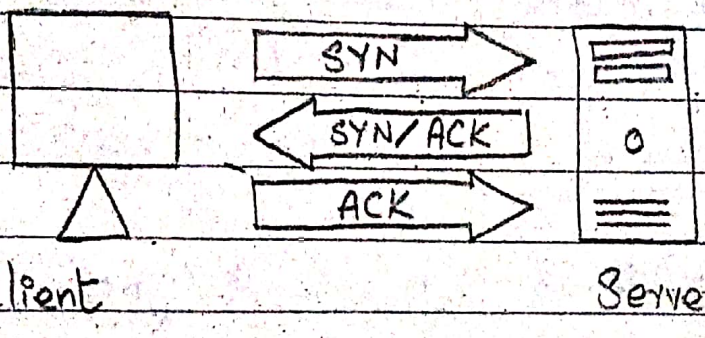


Step no.	N'	X	V	W	Y	Z
0	U	1,U	2,U	5,U	∞	∞
1	UX		2,U	4,X	2,X	∞
2	UXV			4,X	2,X	∞
3	UXVY			3,Y		4,Y
4	UXVYW					4,Y
5	UXVYWZ					

Q#4(a)

Define the three-way handshake for reliable connection establishment and termination that TCP used?

TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps — SYN, SYN-ACK, and ACK.



→ The client chooses an initial sequence number, set in the first SYN packet.

→ The server also chooses its own initial sequence number, set in the SYN/ACK packet.

→ Each side acknowledges each other's sequence number by incrementing it, this is the acknowledgement number.

→ The use of sequence and acknowledgment numbers allows both sides to detect missing or out-of-order segments.

(16)

Q#4(b)

Differentiate b/w the

i) NAT vs PAT

NAT	P
1) NAT stands for "Network Address Translation".	PAT st Transla
2) Private IP addresses are translated into the public IP address.	Private transla IP add
3) NAT can be considered PAT's superset.	PAT i

ii) access routers vs border routers:

Access Router	Border Router
1) It is a hardware device which is responsible for receiving, analyzing and forwarding the data packets to other networks.	Border routers are routers that sit at the edge of the thread network and an external network.
2) It's function is to routing the traffic from one network to the other.	It's function is to provide connectivity of the nodes on the Thread network to other devices in external networks or to the cloud.

iii) Fragmentation and Segmentation.

Fragmentation	Segmentation
1) Fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that resulting pieces can pass through a link with a smaller Maximum Transmission Unit (MTU) than the original packet size.	Segmentation is the process of dividing a data packet into smaller units for transmission over the network.
2) It occurs at layer 3 of OSI Model (Network layer).	It occurs at layer 4 of OSI Model (Transport layer).
3) It is associated with IP	It is associated with TCP.

128 64 32 16 8 4 2 1

(19)

Q#4(c)

For the following, determine the network address and the broadcast address.

i) 15.5.16.35 255.255.255.192

For Network Address:

15 . 5 . 16 . 00100011

255 . 255 . 255 . 11000000

15 . 5 . 16 . 00000000 AND

15 . 5 . 16 . 0 (Network Address)

For Broadcast Address:

15 . 5 . 16 . 00 000000

Network Host

15 . 5 . 16 . 00111111] Broadcast Address

15 . 5 . 16 . 63

128 64 32 16 8 4 2 1

1 0 1 0 1 1 0 0 = 172

0 0 1 0 0 1 1 0 = 38

(20)

ii) 212.172.38.172 255.255.128.0

212.178.00100110.10101100

255.255.10000000.00000000

212.178.00000000.00000000 AND

212.178.0.0 (Network Address)

255.255.10000000.00000000

Network Host

Similarly,

212.178.00000000.00000000

Network Host

212.178.01111111.11111111	Broadcast Address
212.178.127.255	

(21)

128	64	32	16	8	4	2	1	
1	1	0	1	0	1	0	0	= 212
1	0	1	1	1	1	1	1	= 191
1	1	1	0	0	0	0	0	= 224

iii) 108 . 163 . 212 . 191 255 . 255 . 224 . 0

108 . 163 . 11010100 . 10111111

255 . 255 . 11100000 . 00000000

108 . 163 . 11000000 . 00000000 AND

108 . 163 . 192 . 0 (Network Address)

108 . 163 . 11000000 . 00000000

Network Host

108 . 163 . 11011111 . 11111111] Broadcast Address

108 . 163 . 223 . 255