Name: ________________ **Entry Number:** ________________

Mid-term Exam – Solution

COL334/672: Computer Networks

Sem I, 2024-25

There are 19 questions and 17 pages in this quiz booklet (including this page). There are **100 total points**, and you have **120 minutes** to answer the questions.

- **Feel free to think outside the box but write inside the box**
- **Write concise answers**
- **Do not start the exam until instructed to do so**

I Internet Overview

1. [12 points]: True or False. 2 mark each. -1 for wrong answers.

A. Internet is a packet-switched network. **True**

B. Security was one of the built-in design principles of the Internet. **False**

C. A Layer 2 (L2) switch does not modify L2 packet headers while a Layer 3 (L3) switch modifies L3 packet headers. **True**

D. Transport layer is implemented in the hardware. **False**

E. In a link-state routing protocol, each node constructs the same shortest path tree. **False**

F. In a router, the prefix lookup table is in a shared memory accessible to all input ports. **False**

2. [3 points]: Early versions of TCP combined functions for both forwarding and reliable delivery. How are these TCP variants located in the ISO/OSI protocol stack? Why do you think protocol designers decide to separate forwarding functions from TCP?

Solution:

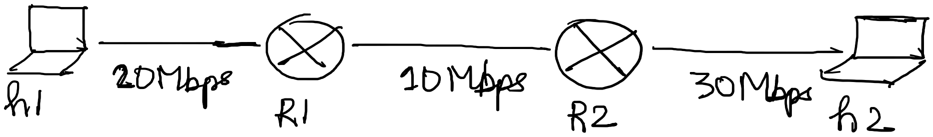
- **Location in the OSI Stack**: Forwarding - Network layer, Reliable delivery- Transport layer.
- **Why?**: Make the design modular. TCP stack and forwarding which is also located in routers could now evolve independently.

3. [4 points]: IIT Delhi's network uses a proxy server on it wired LAN which works by intercepting and modifying the network traffic [both network and transport-layer headers] between client and the Internet.

- List two Internet design principles that are violated by the use of such a proxy server.
- Mention two possible reasons why the network admin might have decided to use a proxy.

Solution:

- **Design principles that are violated**: Layering, end-to-end design principle.
- **Why proxy?**: Authentication, Caching, Security



4. [8 points]: Consider the above network topology. Suppose you send two back-to-back packets, each 1 kbit in size, from h1 to h2.

- Calculate the arrival times of the first and second packet at host h2. Assume that propagation and processing delays are negligible, and there is no cross-traffic.
- Can you sketch a technique to estimate the path capacity using only end-host measurements, i.e., without any knowledge of the network topology as well as the link capacity?

Solution:

- Arrival time for packet 1 is 0.183ms and arrival time for packet 2 is 0.283ms
- Technique: Send packet-pair i.e. two packets back-to-back; Inter-arrival time at the receiver is $\frac{L}{min(C)}$. Ideally, one can send multiple such packet-pairs and use some central measure of the inter-arrival time for a more accurate estimation of path capacity.

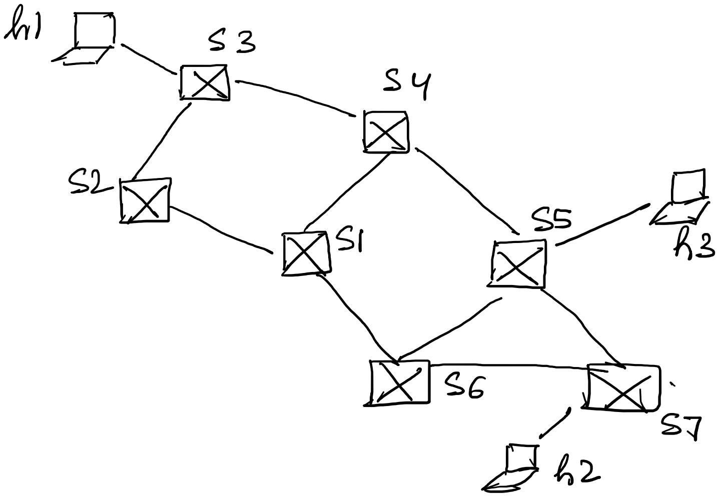
II Link-layer

5. [4 points]: Answer the following questions:

- ∗ Consider a multi-access link with a bandwidth of 100 kbps and a length of 200 km, where nodes use CSMA for medium access. What is the minimum packet size required to ensure that a collision can always be detected? Assume the signal propagates at 2×10^8 m/s in the link.
- ∗ A host decides to send a 1 MB frame over this link. Mention two drawbacks associated with sending such a large frame.

Solution:

- ∗ Minimum Packet size = 200 bits.
- ∗ Drawbacks of sending large frame:
  1. Fairness issues as one user will hog the channel.
  2. Higher probability of bit errors in the frame.



6. [4 points]: MST: What is the spanning tree generated for the following L2 network topology using the *Spanning Tree Protocol?*

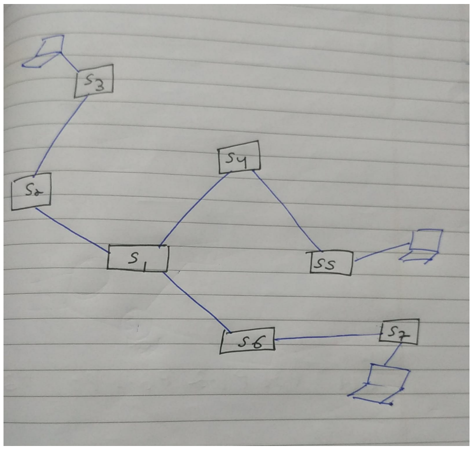


Figure 1: Spanning Tree

7. [6 points]: CRC: Prove that a generator polynomial in CRC can always detect odd number of bit errors, if it has x+1 as one of its factors. [**Hint**: if H(x) divides P(x) then H(1) also divides P(1)]

Solution: Let C(x) be the generator polynomial.
C(x)=(x+1)*C'(x)
Let P(x) be the original msg sent by sender and P'(x) be the msg received by the receiver.
E(x)=P'(x)-P(x)
Error can go undetected iff E(x)% C(x) == 0
if E(x)% C(x) == 0 then E(1)% C(1) == 0
C(1)=(1+1)*C'(x)
C(1)=2*C'(x)
C(1) is even
E(1) = number of bit errors = odd
E(1)%C(1) != 0

8. [7 points]: Slotted Aloha: Consider a multi-access link using the Slotted Aloha protocol with N nodes. Each node has a frame of the same size to send, and each node transmits in a given time slot with probability p.

- What is the probability that a single node successfully transmits its frame in a time slot? This is also termed as efficiency.
- Before the introduction of Slotted Aloha, the Pure Aloha protocol was used, where a node could transmit at any time with probability p. Given the efficiency of Slotted Aloha is $\frac{1}{e}$ as $N \to \infty$, What is the efficiency of Pure Aloha? [**Hint**: Consider the vulnerable period, i.e. the period during which collision can occur, in Pure Aloha compared to Slotted Aloha.]

Solution: Slotted Aloha:
P(successful transmission by 1 node) = $p * (1 - p)^{N-1}$
P(successful transmission by any node) = $N * p * (1 - p)^{N-1}$
Pure Aloha:
let T be the time taken to transmit a frame (also the slot size)
if the current node transmits as t0, no other node should have transmitted in [t0 -T, t0] and no other node should transmit in [t0, t0 + T]
Therefore, the vulnerable period is twice of the vulnerable period of Slotted Aloha.
Hence, efficiency is reduced to half of Slotted Aloha, i.e., $\frac{1}{2e}$

9. [6 points]: Wireless MAC protocol

- Explain how CSMA/CA addresses the hidden terminal problem.
- *Exposed terminal problem*: Consider a network with four wireless nodes: A, B, C, and D. A and B can hear each other, B and C can hear each other, and C and D can hear each other. B and C want to send data to A and D, respectively. Can these two nodes transmit simultaneously using CSMA/CA? Explain your reasoning.

Solution:

- CSMA/CA uses control signals:
  - RTS(request to send): If a node wants to transmit it will send this signal to the desired reciever.
  - CTS(clear to send): The reciever sends clear to send indicating the channel is free, the reciever broadcasts the CTS so that the other nodes nearby listening to it stops there transmission and wait until the line is free.

  Even if two hosts send RTS simultaneously in the hidden terminal case, only one of them will receive the CTS. Hence, it solves the hidden terminal problem.
- B sends the RTS to A and gets the CTS from A similarly C sends the RTS to D and gets the CTS from D, Now because C is out of reach from A and B is out of reach from D, terminal C doesn't hear the CTS from A hence it can trasnmit in that channel similarly terminal B cannot hear the CTS from D and it can also transmit in that channel. Hence, simultaneous transmission can happen.

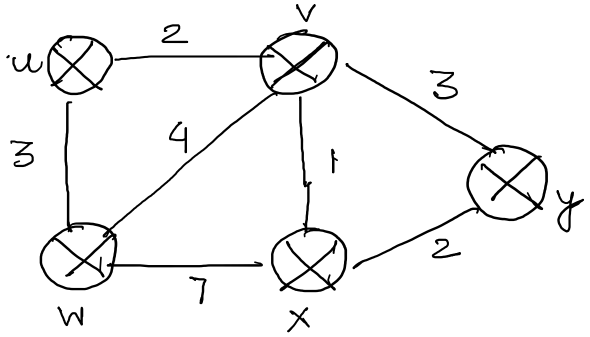
III Network-layer

10. [4 points]: IPv6: Answer the following

- What was the main motivation for designing IPv6 when IPv4 already existed? Explain the change in the IPv6 protocol that address the limitation of IPv4.
- Explain why the designers of IPv6 decided not to include a checksum header.

Solution:

- IPv4 used 32-bit addresses which were quickly running out as the Internet-connected devices grew. Therefore, IPv6 was designed which uses a 128-bit address space, offering a much larger address space.
- Transport Layer already uses checksum for error detection. Similarly, Data Link Layer has CRC for error detection. Hence, to reduce the redundancy, the designers removed the checksum from the IPv6.



11. [4 points]: Consider the network shown to the left. Assume that each node initially knows the costs to each of its neighbors. Consider link-state routing algorithm and show how shortest path tree is calculated at node *y* as well as the final routing table.

Step	N’	D(u), p(u)	D(v), p(v)	D(w), p(w)	D(x), p(x)
0	y	∞	(3, y)	∞	(2, y)
1	y,x	∞	(3, y)	(9, x)	(2, y)
2	y,x,v	(5, v)	(3, y)	(7, v)	(2, y)
3	y,x,v,u	(5, v)	(3, y)	(7, v)	(2, y)
4	y,x,v,u,w	(5, v)	(3, y)	(7, v)	(2, y)

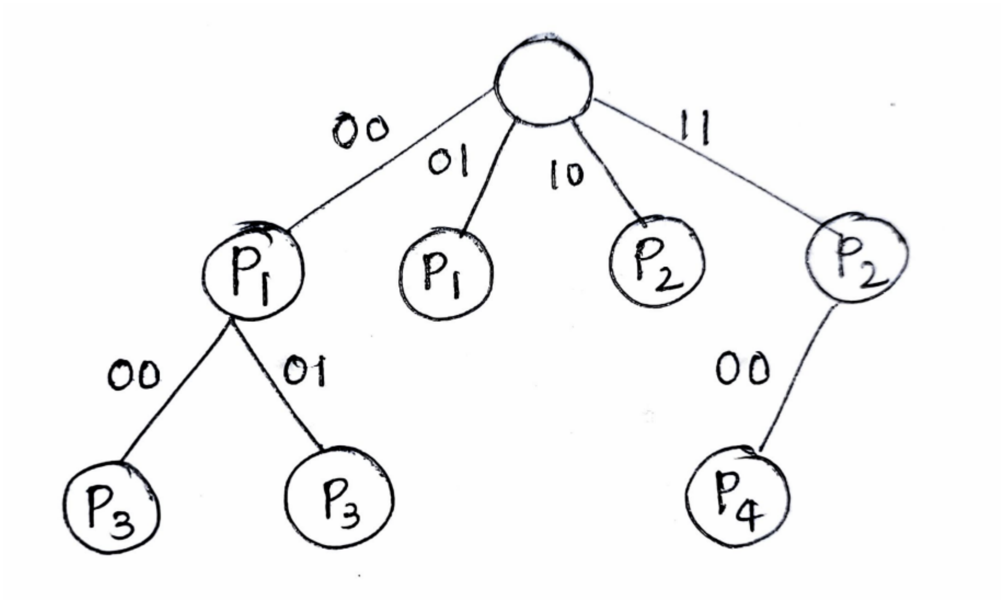
Table 1: Using Dijkstra’s algorithm to find shortest path from node ’y’

Destination	Next hop	Cost
u	v	5
v	v	3
w	v	7
x	x	2

Table 2: Final routing table

12. [4 points]: You got a new router, called router X, which uses a 2-bit trie for prefix lookup. How would the trie look like for the following prefix table?

IP Prefix	Port
0*	1
1*	2
000*	3
1100*	4



13. [6 points]: Answer the following questions:

- What is head-of-line blocking in packet switching? How can you address it?
- List two drawbacks of having larger buffer size in routers?

Solution:

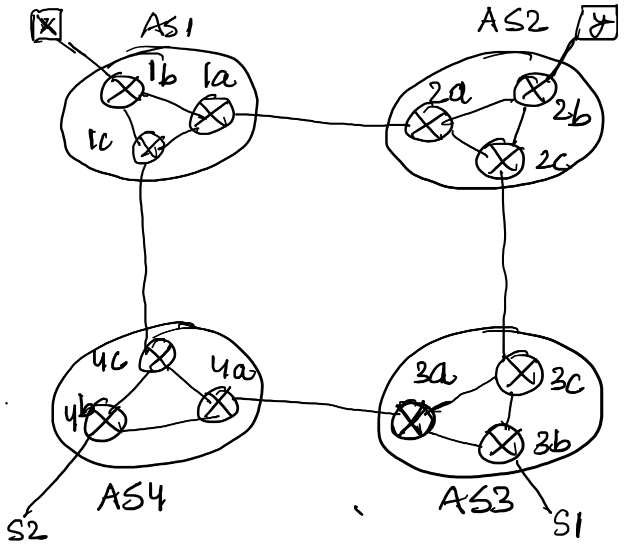
- Head of Line Blocking: It happens when a packet at front of a queue prevents other packets in the queue from being transmitted, even if the output ports of those packets are free/idle, This happens because the output port of the front packet is already busy/occupied.
- Address HOL: Virtual Output Queues (VOQ)- Implementing VOQs where each input port maintains separate queues for each output port. This prevents a packet destined for one output port from blocking packets destined for other output ports.
- Drawbacks of having large buffer size in routers: Bufferbloat or high latency, High jitter, higher memory requirement.

14. [3 points]: Consider three hosts, each subscribed to different bandwidth plans from an ISP: 10 Mbps, 30 Mbps, and 60 Mbps. If the ISP has a 100 Mbps link and each host is sending a large file, how can the ISP ensure that each host receives the bandwidth they are subscribed to?

Solution: Use Weighted Fair Queuing (WFQ) at an aggregation router. E.g., the router connected to the bottleneck link. The ISP can assign weights to each host based on their subscription plan which is in the ratio of 1:3:6.
The bandwidth share of each host will be:

$$\text{Bandwidth Share}_i = \frac{W_i}{\text{Total Weight}} \times 100$$

- **NOTE:** TDMA or FDMA have been awarded partial marks as the bottleneck link could be anywhere in the network and using TDMA/FDMA may not be feasible always.



15. [5 points]: BGP: Content providers like Google sometimes use *IP Anycast* to route data to the closest server based on network topology. In IP anycast, multiple servers are configured with the same IP address, referred to as the anycast address. Each server advertises this address as BGP announcements to the network. Consider the network topology shown in the figure, where S1 and S2 are anycast servers advertising a common IP address, and *x* and *y* are two hosts attempting to connect to the anycast IP:

- Show the flow of BGP announcements and explain which path each host will select.
- Can AS1 force *x* to connect to S1? If so, how?

Solution: **Part1**: Assuming anycast IP is Z. Then,
1c receives *AS4* $Nxt\_hop(4c)$ *Z*
1a receives *AS2 AS3* $Nxt\_hop(2a)$ *Z*
1b receives *AS4* $Nxt\_hop(1c)$ *Z* and *AS2 AS3* $Nxt\_hop(1a)$ *Z* from 1c and 1a, respectively.
1a selects the announcement from 1a as it has lower number of AS hops. Hence, x will connect to S2. Similar is the case for y and it will connect to S1.
Part 2: Yes. AS1 can set a higher $local\_pref$ value to the announcement received from 1a.

IV Software-defined Network

16. [4 points]: Each technology typically has some factors that drive its adoption (often referred to as 'pull' factors) and some factors that promote its development or advancement (often referred to as 'push' factors). What were the 'pull' and 'push' factors for Software-Defined Networking (SDN)?

Solution:

Pull factors for SDN:

- Traffic Management, Deploying new routing applications, Managing Interoperability between various OEMs/Models, etc.

Push factors for SDN:

- Switch vendors had started opening up switch APIs to allow programmers to control certain forwarding behavior, etc.

17. [4 points]: What is network function virtualization? Give two benefits of NFV.

Solution:

NFVs:

- Making middleboxes programmable by running network fuctions in the software (typically as virtual machines) on commodity hardware.

Benefits of NFVs:

- Removes the need to have a specialized hardware for each middlebox leading to faster deployment and innovation
- consolidation of hardware boxes in the network
- increases flexibility/programmability.

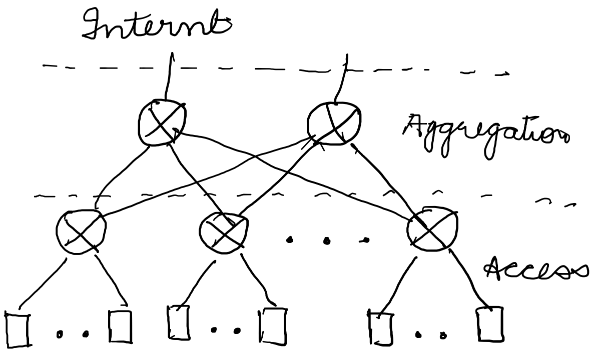
18. [4 points]:

- How is a Protocol Independent Switch Architecture (PISA) able to support new packet protocols?

- A PISA switch is able to obtain similar performance as a traditional switch while providing programmability in data plane. How is this possible?

Solution:

- PISA introduces a programmable parser that can be used to support new packet protocols.
- Traditional switches implemented a lot of redundant functionalities which made their design bloated. PISA removed it using its programmable parser, which overcame the space-tradeoff, thereby providing programmability in data plane, while simultaneously providing similar performance as a traditional switch.



19. [8 points]: You are the network architect at a data center network with the given topology. There are two layers: *access layer* that connects servers to the network and *aggregation layer* that connects switches in the access layer with each other. There are 100s of server connected to each access-layer switch and 100s of access-layer switches and two aggregation switches. In a traditional network, these all can be L3 switches. However, you are asked to implement a L2 topology (for performance reasons), which means that forwarding needs to be done using MAC addresses as all machines are in the same subnet. Another constraint is that the server software and NIC can not be modified.

- Can you identify a challenge with L2-based forwarding in this large network?

- Sketch a system that uses SDN for addressing the above challenge. [Hint: You will need to handle ARP requests from these servers too]

Solution: **Challenge**: MAC addresses are flat. The forwarding tables at the aggregation switch will be large, leading to forwarding delays.
Approach: Use pseudo-MAC. Each subtree connected to access switch could be assigned a hierarchical MAC address. For instance, hosts in subtree-1 could be assigned MAC addreses $01:00:00:00:00:01$ and $01:00:00:00:00:02$.
How to map real MAC to pseudo-MAC given hosts are unmodified?: By intercepting ARP requests at the access switch. Each ARP request at the access switch can be sent to an SDN controller which will respond with the pseudo-MAC for a given IP address. Once, a packet reaches at the destination access switch, the access switch will translate back the psuedo-MAC (using MODIFY ACTION) to the real MAC address and forward it to the host.