CS 348: Computer Networks
Spring 2025, IIT Dharwad

End-semester Exam
May 3, 2025

09:30 AM to 12:30 PM
Total Marks: 91

Name: _____ **Roll No.** _____

Instructions

- This is a question paper-cum-answer sheet, which must be submitted to the invigilator at the end of the exam.
- Answers are to be written exclusively in the space provided after each question.
- Extra sheets may be used for rough work, which need not be submitted.
- No notes, books, cheat-sheet, calculator, etc. are allowed in this exam.
- One or more option(s) may be correct for all MCQs. Full marks will be awarded only if all correct options are selected. No partial marks will be awarded in such questions.

Q1. [1 mark] The Internet was originally developed as a commercial project by private tech companies. True or False.

Ans. False
Explanation: The Internet originated from a U.S. Department of Defense project called ARPANET in the late 1960s.

Q2. [1 mark] TCP slow start increases the congestion window (cwnd) linearly with each round-trip time. True or False.

Ans. False. In slow start, the congestion window increases exponentially, doubling each RTT until a threshold is reached.

Q3. [1 mark] The SDN control plane is physically centralized. True or False.

Ans. False

Q4. [1 mark] Network-assisted congestion control requires cooperation from routers or switches in the network. True or False.

Ans. True.

Q5. [1 mark] Which of the following is considered a host in a computer network?

a. Ethernet cable b. Wi-Fi router c. Smartphone d. Optical fiber

Ans. c
Explanation: A host is any end device that sends or receives data across the network, such as a smartphone, computer, or server.

Q6. [1 mark] Which of the following is not a typical component of nodal delay in a packet-switched network?

a. Processing Delay
b. Queuing Delay
c. Congestion Delay
d. Transmission Delay

Ans. c
Explanation: Nodal delay typically includes processing, queuing, transmission, and propagation delays. Congestion affects queuing delay but is not a distinct component.

Q7. [1 mark] Which field is present in the TCP header but absent in the UDP header?

a. Source Port b. Destination Port c. Sequence Number d. Length

Ans. c
Explanation: TCP is connection-oriented and uses a sequence number for reliable data transfer. UDP, being connectionless, does not.

Q8. [1 mark] What is the primary purpose of an HTTP Conditional GET request?

a. To send data to the server
b. To request a resource only if it has changed since the last request
c. To authenticate the user
d. To close the connection after the request

Ans. b
Explanation: The primary purpose of a Conditional GET is to minimize bandwidth usage by fetching a resource from the server only if it has been modified since the last request.

Q9. [1 mark] What is the primary purpose of the Internet checksum in TCP/IP?

a. To encrypt the data payload
b. To detect errors in transmission
c. To compress packet headers
d. To perform flow control

Ans. b
Explanation: The Internet checksum is used to detect transmission errors by computing a one's complement sum of the data.

Q10. [1 mark] Two-dimensional parity can _____ single-bit errors and _____ double-bit errors.

a. detect, detect
b. detect, correct
c. correct, detect
d. correct, correct

Ans. c

Q11. [1 mark] In a router, head-of-line blocking may occur at _____ port(s).

a. Input
b. Output
c. Input and output
d. None of these

Ans. a

Q12. [1 mark] Which of the following is the primary role of the OpenFlow protocol in SDN?

a. To encrypt communication between routers and switches
b. To allow the SDN controller to program the flow tables on network switches
c. To define how switches communicate with each other
d. To manage IP address allocation in an SDN network

Ans. b
Explanation: The OpenFlow protocol enables the SDN controller to manage and update the flow tables on switches, providing centralized control of how traffic is forwarded in the network. It allows the controller to dynamically adjust the flow of packets based on the network's current conditions and policies.

Q13. [1 mark] Which of the following OpenFlow messages is used by a switch to send a packet to the controller because it does not match any flow entries?

a. Flow-Mod
b. Packet-In
c. Packet-Out
d. Flow-Stats-Request

Ans. b
Explanation: When a switch receives a packet that does not match any of its existing flow entries, it sends a Packet-In message to the SDN controller. This informs the controller about the unmatched packet, allowing the controller to decide how to handle it.

Q14. [1 mark] Which forwarding technique allows routers to inspect multiple header fields for making forwarding decisions?

a. Distance Vector Routing
b. Generalized Forwarding
c. Link State Routing
d. Destination-Based Forwarding

Ans. b

Q15. [1 mark] In Layer-2 switches, the network interface(s) has/have:

a. MAC Address only
b. IP Address only
c. Both IP and MAC Addresses
d. None of these

Ans. d

Q16. [1 mark] According to RFC 5681, which of the following best describes the purpose of TCP's delayed acknowledgement mechanism?

a. To reduce retransmission timeout values.
b. To acknowledge every received segment immediately to avoid packet loss.
c. To reduce the number of ACK packets by delaying acknowledgements for a short time.
d. To prioritize acknowledgment of control packets over data packets.

Ans. c

Q17. [1 mark] Which of the following best describes the primary purpose of TCP Fast Retransmit?

a. To reduce the size of the congestion window
b. To recover lost packets more quickly than waiting for a timeout
c. To ensure all packets are acknowledged
d. To reset the TCP connection after packet loss

Ans. b

Q18. [1 mark] How does the TCP sliding window mechanism support flow control?

a. By determining when to retransmit lost packets
b. By limiting the amount of unacknowledged data sent by the sender
c. By specifying packet order to avoid reordering
d. By ensuring only one segment is sent at a time

Ans. b

Q19. [1 mark] Why is a two-way handshake insufficient for reliable connection establishment in TCP?

a. It does not allocate buffer space
b. It cannot ensure both parties are ready to transmit and receive
c. It may result in half-open connections
d. It requires an extra round-trip time

Ans. c

Q. [1 mark] What mechanism does QUIC use to handle packet loss more efficiently compared to TCP?

a. QUIC retransmits all packets in a single stream, causing head-of-line blocking.
b. QUIC uses stream-based multiplexing, allowing independent recovery of streams and preventing head-of-line blocking.
c. QUIC waits for a timeout before retransmitting any lost packets.
d. QUIC retransmits all packets, including those that were not lost, to ensure no delay.

Ans. b
QUIC's stream-based multiplexing allows it to recover from packet loss in individual streams without affecting others, thus preventing head-of-line blocking that occurs in TCP.

Q20. [1 mark] Which of the following best describes the best-effort service model provided by the TCP/IP network layer?

a. Guarantees packet delivery and order
b. Ensures low latency and high throughput
c. Delivers packets with no guarantees on delivery, order, or timing
d. Uses acknowledgments and retransmissions for reliability

Ans. c

Q21. [1 mark] Which of the following is the primary difference between eBGP and iBGP?

a. eBGP is used within an AS, while iBGP is used between different ASes
b. iBGP updates routes between routers in the same AS, while eBGP is used between different ASes
c. eBGP uses a cost metric, while iBGP does not
d. iBGP uses an AS path attribute, while eBGP does not

Ans. b

Q22. [1 mark] What is the main principle behind Hot Potato Routing?

a. Always forward the packet to the router with the highest bandwidth
b. Always forward the packet to the router that has the lowest cost to the destination
c. Always forward the packet to the next-hop router as quickly as possible
d. Always forward the packet to the router that minimizes congestion

Ans. c

Q23. [1 mark] Which of the following statements accurately contrasts convergence behavior between Link State and Distance Vector routing protocols?

a. Distance Vector protocols converge faster because updates are shared with all nodes directly.
b. Link State protocols converge faster due to flooding and local computation of shortest paths.
c. Both protocols converge at the same rate if the topology changes are minor.
d. Link State protocols never require periodic updates, unlike Distance Vector.

Ans. b
Link State protocols converge faster because routers receive complete network information via flooding and compute routes locally using Dijkstra's algorithm. Distance Vector protocols rely on incremental updates between neighbors, making convergence slower.

Q24. [1 mark] Which of the following statements accurately describe the relationship between policy-based routing and performance-based routing in BGP?

a. Policy-based routing in BGP can prioritize business objectives over optimal network performance
b. Performance-based routing in BGP ensures that traffic always follows the shortest path
c. Policy-based routing may cause performance degradation if the policies do not align with the best routing paths
d. Performance-based routing in BGP relies exclusively on shortest path calculations and disregards any administrative rules

Ans. a, c
Explanation:
a: True – Policy-based routing can enforce business or administrative decisions (e.g., routing through a certain AS) at the expense of performance.
b: False – Performance-based routing typically aims to find optimal routes (e.g., shortest path, lowest latency), but it doesn't always guarantee shortest path if the policy dictates otherwise.
c: True – Policy-based routing might cause performance degradation since the policies may dictate suboptimal routes.
d: False – Performance-based routing typically tries to optimize for performance but may still take into account certain administrative rules in BGP.

Q25. [1 mark] Which of the following are true about the interaction between policy, shortest path, and hot potato routing in BGP decision-making?

a. Hot Potato Routing always takes precedence over policy-based routing if a tie occurs.
b. Shortest path is always preferred if no specific policy constraints exist.
c. Policy can dictate which path is preferred even if it is not the shortest.
d. Hot Potato Routing considers both performance metrics like bandwidth and latency when selecting the path.

Ans. b, c
Explanation:
a: False – Hot Potato Routing does not always take precedence. It only comes into play when routes are tied and can't be distinguished based on policy or shortest path alone.
b: True – When no specific policies are applied, BGP selects the shortest path based on attributes like AS path length, weight, or cost.
c: True – Policy is often the primary deciding factor in BGP when determining the best path. If policy conflicts with shortest path, the policy will usually override.

d: False – Hot Potato Routing primarily focuses on getting the packet out of the network quickly and does not consider latency or bandwidth in its decision-making process.

Q26. [1 mark] Which of the following statements are true for Slotted ALOHA?
a) It requires time synchronization across all users
b) It allows for overlapping transmissions
c) The efficiency of Slotted ALOHA is higher than that of Pure ALOHA
d) The maximum throughput of Slotted ALOHA is 100% of the channel capacity

Ans. a, c
Explanation:
a) True – Slotted ALOHA requires all users to synchronize their transmissions to time slots.
b) False – Overlapping transmissions are not avoided in Slotted ALOHA.
c) True – Slotted ALOHA has higher efficiency than Pure ALOHA because it reduces collisions by allowing only one transmission per time slot.
d) False – The maximum throughput of Slotted ALOHA is 36.8% of the channel capacity.

Q27. [1 mark] Which of the following statements are true about MAC addresses and IP addresses?
a. MAC addresses are used for communication between devices on different networks
b. MAC addresses are assigned by manufacturers, while IP addresses can be assigned by network administrators
c. IP addresses can be changed as devices move between different networks, but MAC addresses remain the same
d. MAC addresses are assigned dynamically by a network's DHCP server

Ans. b, c
Explanation:
a) False – MAC addresses are used for communication within a local network, not between different networks.
b) True – MAC addresses are hardcoded by the manufacturer, while IP addresses can be statically or dynamically assigned by network administrators or DHCP servers.
c) True – IP addresses can change as devices move between networks, while MAC addresses remain static unless altered by software.
d) False – MAC addresses are assigned by manufacturers and do not change dynamically through DHCP. IP addresses, however, are assigned dynamically via DHCP.

Q28. [1`mark] Which of the following statements are true about how ping and traceroute use ICMP?
a. ping sends an Echo Request message and waits for an Echo Reply to check if a host is reachable.
b. ping sends an Echo Request message to each router along the path to check each hop's status.
c. traceroute uses Time Exceeded messages to trace the path by incrementing the TTL value on successive packets.
d. traceroute uses Echo Reply messages to trace the path taken by packets to the destination.

Ans. a, c
Explanation:
a) True: ping uses Echo Request to check host reachability and waits for the Echo Reply to confirm the host is responding.
b) False: ping does not send messages to each router along the path. It only sends Echo Request to the destination.
c) True: traceroute uses Time Exceeded messages by incrementing the TTL value for each successive packet, causing routers along the path to send these messages when the TTL expires.
d) False: traceroute does not rely on Echo Reply messages for tracing the path; it uses Time Exceeded messages.

Q29. [1 mark] Which of the following are true about HTTP response message format?
a. The first line contains the HTTP method used by the client.
b. The response body may contain data like HTML, images, or JSON.
c. The status code in the response tells the server's status.
d. The response headers contain information like server type and content type.

Ans. b, d

Explanation: The first line of an HTTP response message contains the status line, not the HTTP method. The body of the response contains the data sent by the server (e.g., HTML, images, JSON). Response headers include metadata about the response, such as the server type and content type.

Q30. [1 mark] Which of the following are advantages of the BitTorrent protocol over traditional client-server file distribution?

a. Faster downloads due to parallel transfers from multiple peers
b. Centralized control over the distribution process
c. Reduced strain on the server hosting the files
d. Encryption of file transfers

Ans. a, c
Explanation:
a. In BitTorrent, the file is divided into small pieces that can be downloaded in parallel from multiple peers, significantly speeding up the overall download time.
c. Because the file is distributed across many peers, there is less reliance on a central server, reducing the strain on the server that would otherwise serve the file to each downloader.
b. BitTorrent is decentralized, so there is no centralized control; it's distributed across many peers, which is a key difference from traditional client-server systems.
d. BitTorrent does not inherently provide encryption for file transfers (though encryption can be added via specific clients or settings).

Q31. [1 mark] Which of the following are benefits of using the DASH protocol for video streaming?

a. It allows video streaming to be delivered over HTTP, which can traverse firewalls easily
b. It provides fixed video quality, regardless of the viewer's bandwidth
c. It supports adaptive streaming, ensuring smooth playback despite network fluctuations
d. It requires proprietary player support for playback

Ans. a, c
Explanation:
A. DASH uses HTTP for delivering video, making it easier to traverse firewalls and work with existing HTTP infrastructure.
C. One of the key features of DASH is its ability to adapt to changing network conditions by adjusting the video bitrate and quality, ensuring uninterrupted playback.
B. DASH does not provide fixed video quality; it adapts the quality based on available bandwidth.
D. DASH is designed to work with a wide range of players, as it is an open standard and does not require proprietary player support.

Q32. [1 mark] Which of the following are true about persistent HTTP?

a. It allows for better resource utilization.
b. It reduces latency by eliminating the need for multiple TCP handshakes.
c. It automatically closes the connection after each HTTP request.
d. It is only applicable for HTTP/1.1 or higher.

Ans. a, b, d
Explanation: Persistent HTTP helps reduce overhead, but it is mainly available in HTTP/1.1 and beyond. It does not automatically close the connection after each request; it is kept open for further communication.

Q33. [1 mark] Which of the following are advantages of packet switching over circuit switching?

a. Efficient use of bandwidth
b. Guaranteed delivery time
c. Greater scalability
d. Lower cost for bursty traffic

Ans. a, c, d
Explanation: Packet switching is more efficient for bursty data, supports many users, and scales well. It does not guarantee delivery time.

Q34. [1 mark] Which of the following statements are true about interconnection networks in routers?

a. They enable concurrent transfers if input-output pairs don't conflict
b. They completely eliminate the need for buffering
c. They are more complex to design than memory- or bus-based fabrics
d. They can be implemented using crossbars, Clos networks, or multistage switches

Ans. a, c, d

Q35. [1 mark] What information can a DHCP server provide to a client, apart from an IP address?

a. Subnet Mask
b. Default Gateway
c. DNS Servers
d. MAC Address of the Gateway

Ans. a, b, c

Q36. [1 mark] Which of the following are valid distinctions between intra-ISP and inter-ISP routing protocols?

a. Intra-ISP protocols usually converge faster than BGP
b. BGP routes are influenced by policy rather than shortest path
c. RIP and OSPF use AS-path as their routing metric
d. Inter-ISP protocols must consider scalability and policy compliance

Ans. a, b, d
Explanation:
A: True – OSPF/EIGRP converge faster than BGP
B: True – BGP allows routing based on business policies
C: False – AS-path is used in BGP, not RIP/OSPF
D: True – BGP is built for scalability and policy control between large networks

Q37. [1 mark] Which of the following are limitations of traditional traffic engineering (without SDN) compared to SDN-based traffic engineering?

a. Traditional routing protocols rely on local views of the network, which can lead to suboptimal path selection.
b. In traditional networks, it is difficult to perform real-time traffic optimization.
c. SDN-based traffic engineering requires no monitoring of network state.
d. SDN provides global network visibility for dynamic path adjustments.

Ans. a, b, d
Explanation:
a: True – Traditional routing protocols only have local views of the network and rely on periodic updates, which can lead to suboptimal routing decisions.
b: True – Traditional networks often cannot dynamically optimize traffic flows in real-time as changes are slow to propagate across the network.
c: False – SDN still requires monitoring and collecting data from the network to make real-time decisions, unlike traditional networks that rely on manual monitoring.
d: True – SDN provides global network visibility, allowing it to adjust traffic dynamically across the entire network based on real-time data.

Q38. [1 mark] Which of the following are key challenges faced by SDN controllers?

a. High computational power requirements for the centralized controller
b. Lack of flexibility in managing dynamic network conditions
c. Security vulnerabilities due to centralized control
d. Increased overhead due to real-time network monitoring and decision-making

Ans. a, c, d
Explanation:
a: The SDN controller needs significant computational resources to manage the entire network, especially for large-scale deployments, which can be a challenge in terms of scalability and performance.

b is incorrect because SDN itself provides high flexibility, allowing dynamic network management in response to changing conditions, which is one of its key advantages.
c: Centralized control introduces the risk of a single point of failure and can become a security vulnerability if the controller is compromised.
d: The real-time monitoring and dynamic decision-making required by SDN controllers add processing overhead, which could affect performance in high-speed, large-scale networks.

Q39. [1 mark] Which of the following conditions can lead to packet loss at the input port of a router?

a. Switching fabric cannot transfer packets to the output port fast enough
b. Output port queue is full due to congestion
c. Packets arrive faster than they can be moved into the switching fabric
d. Input buffer size is insufficient during fabric contention

Ans. a, c, d
Explanation:
(a) and (c) both reflect conditions where the switching fabric becomes a bottleneck for transferring packets, causing input-side buffer buildup.
(d) Small or constrained input buffers can exacerbate packet loss during high contention.
(b) Output congestion affects the output port, not the input.

Q40. [1 mark] Which of the following are true about channel partitioning protocols such as TDMA and FDMA?

a. They avoid collisions by design
b. They offer high utilization under bursty traffic
c. They require synchronization or frequency coordination
d. They do not adapt well to dynamic user demand

Ans. a, c, d
Explanation:
a) True – Collision is avoided by assigning distinct slots or frequencies.
b) False – Fixed allocation results in inefficiencies during bursty traffic.
c) True – Synchronization (TDMA) and coordination (FDMA) are required.
d) True – Static resource allocation limits adaptability to changing traffic loads.

Q41. [1 mark] Which of the following are characteristics of CSMA/CD?

a. It requires the sender to sense the channel before transmitting
b. It uses a fixed time slot for every transmission
c. It stops transmission immediately upon detecting a collision
d. It can be more efficient than CSMA in terms of collision handling

Ans. a, c, d
Explanation:
a) True – CSMA requires the sender to sense the channel before transmission to avoid collisions.
b) False – CSMA/CD does not use time slots; it relies on sensing and collision detection.
c) True – If a collision is detected, CSMA/CD immediately stops transmission and attempts retransmission.
d) True – CSMA/CD is more efficient in collision management because it detects and addresses collisions faster than CSMA.

Q42. [1 mark] Which of the following statements about ARP are true?

a. ARP is used to resolve IP addresses to MAC addresses in a local network
b. ARP operates only within the same subnet
c. ARP requests are sent as unicast packets to the destination IP address
d. Devices can cache ARP responses for future use to avoid sending repeated ARP requests

Ans. a, b, d
Explanation:
a) True – ARP resolves IP addresses to MAC addresses within a local network.

b) True – ARP operates within the same subnet (local network).
c) False – ARP requests are broadcast to all devices in the local network, not unicast.
d) True – ARP responses are cached for a period of time to avoid frequent ARP requests.

Q43. [1 mark] Which of the following are valid motivations for using generalized forwarding instead of destination-based forwarding?

a. Traffic engineering based on real-time network load
b. Enforcing user-level access policies
c. Differentiating traffic based on protocol and port number
d. Supporting multi-tenant data center traffic isolation

Ans. a, b, c, d

Q44. [1 mark] Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are R_1 and R_2, respectively. If the switch uses store-and-forward packet switching, what is the total end-to-end delay to send a packet of length L? (Ignore queuing, propagation delay, and processing delay.)

Ans. $\frac{L}{R_1} + \frac{L}{R_2}$

Explanation: At time t_0, the sending host begins to transmit. At time $t_1 = \frac{L}{R_1}$, the sending host completes transmission, and the entire packet is received at the router (no propagation delay). Because the router has the entire packet at time t_1, it can begin to transmit the packet to the receiving host at time t_1. At time $t_2 = t_1 + \frac{L}{R_2}$, the router completes transmission, and the entire packet is received at the receiving host (again, no propagation delay). Thus, the end-to-end delay is $\frac{L}{R_1} + \frac{L}{R_2}$.

Q45. [1 mark] What advantage does a circuit-switched network have over a packet-switched network?

Ans. Guaranteed delay and bandwidth
Explanation**:** A circuit-switched network can guarantee a certain amount of end-to-end bandwidth for the duration of a call. Most packet-switched networks today (including the Internet) cannot make any end-to-end guarantees for bandwidth.

Q46. [1 mark] How is the IPv6 checksum calculated?

Ans. There is no checksum in IPv6.

Q47. [2 marks] In CSMA/CD, after the fifth collision, what is the probability that a node chooses K = 4? The result K = 4 corresponds to a delay of how many seconds on a 10 Mbps Ethernet?

Ans. After the 5th collision, the adapter chooses from {0, 1, 2, …, 31}. The probability that it chooses 4 is 1/32. It waits 204.8 microseconds.

Q48. [2 marks] Consider the 5-bit generator, G = 10011, and suppose that D has the value 1010101010. What is the value of R?

Ans. If we divide 10011 into 1010101010 0000, we get 1011011100, with a remainder of R=0100.

Q49. [2 marks] Match each TCP variant with its key characteristic:

TCP Variant	Key Characteristic
A. Tahoe	1. Proactively adjusts window using RTT estimates
B. Reno	2. Reduces window by half and avoids full reset
C. Vegas	3. Uses exponential growth followed by drop to 1
D. Cubic	4. Window growth decelerates after plateauing

Ans. A-3, B-2, C-1, D-4

Q50. [2 marks] Match each term with its correct description:

Term	Description
A. Control Plane	1. Chooses packet forwarding paths using routing protocols
B. Data Plane	2. Forwards packets based on routing table entries
C. Routing	3. Global process for path computation
D. Forwarding	4. Local per-router process for sending packets out an interface

Ans. A-1, B-2, C-3, D-4

Q51. [2 marks] Match each SNMP/NETCONF term with its correct description:

Term	Description
A. SNMP Agent	1. Executes operations on a network device as per configuration requests
B. NETCONF Client	2. Receives and logs information from devices for monitoring purposes
C. YANG Model	3. Schema for defining the structure of configuration data
D. SNMP Manager	4. Resides on a managed device and provides access to MIB data

Ans. A–4, B–1, C–3, D–2

Q52. [2 marks] A router receives a packet with destination IP 192.168.12.77. Its forwarding table contains the following entries:

Prefix	Next Hop
192.168.12.0/24	A
192.168.12.128/25	B
192.168.12.64/26	C
192.168.12.32/27	D

Which next hop will be chosen?

Ans. C

Q53. [2 marks] Match each TCP/IP layer with its primary responsibility:

Layer	Responsibility
A. Transport	1. Defines protocols like HTTP/FTP
B. Application	2. IP addressing and routing
C. Link	3. Reliable delivery, segmentation
D. Internet	4. Physical addressing, MAC frames

Ans. A–3, B–1, C–4, D–2

Q54. [2 marks] Match each protocol with its correct layer in the Internet protocol stack:

Protocol	Layer
A. IP	1. Application Layer
B. HTTP	2. Network Layer
C. TCP	3. Transport Layer
D. DNS	

Ans. A–2, B–1, C–3, D–1

Q55. [2 marks] Match the technology with its role in the history of the Internet:

Technology	Role
A. ARPANET	1. Foundation for Internet protocol stack
B. TCP/IP	2. Government-funded research network
C. DNS	3. Translates domain names to IP addresses

Ans. A–2, B–1, C–3

Q56. [2 marks] Match the following TCP header fields with their function:

Field	Function
A. Sequence Number	1. Advertises how much data can be received
B. Acknowledgment Number	2. Identifies the next expected byte
C. Window Size	3. Tracks the byte position of sent data
D. Flags (e.g., SYN, ACK)	4. Controls connection setup and teardown

Ans. A–3, B–2, C–1, D–4
Explanation: Each field is crucial to TCP's reliability and connection-oriented behavior. Flags like SYN and ACK are used during connection establishment and termination.

Q57. [2 marks] You are designing a routing protocol for a network with 1000 routers and 3000 links. If minimizing message overhead is critical, which algorithm is more suitable: Dijkstra (Link-State) or Bellman-Ford (Distance Vector)? Justify your choice in terms of message complexity.

Ans. Bellman-Ford (Distance Vector) is more suitable.
Justification:
- Bellman-Ford only requires routers to exchange information with their direct neighbors, resulting in O(E) message complexity over each iteration.
- Dijkstra's algorithm, as used in Link-State routing, requires global dissemination of topology updates (via flooding), leading to higher message complexity, especially when topology changes are frequent.

Q58. [2 marks] Consider the following graph:

- A → B (weight = 4)
- A → C (weight = 1)
- C → B (weight = 2)
- B → D (weight = 1)
- C → D (weight = 5)

Using Dijkstra's algorithm, what is the shortest path from A to D, and its cost?

Ans. Shortest path: A → C → B → D. Total cost = 1 + 2 + 1 = 4.

Q59. [2 marks] Suppose Host A sends two TCP segments back-to-back to Host B over a TCP connection. The first segment has sequence number 90; the second has sequence number 110.

a. How much data is in the first segment?
b. Suppose that the first segment is lost but the second segment arrives at B. In the acknowledgment that Host B sends to Host A, what will be the acknowledgment number?

Ans. (a) 20 bytes (b) 90

~~**Q60.** [2 marks] An incoming packet header matches multiple forwarding/flow table entries at a switch. How to break the ties in case of:~~

~~a. Destination-based forwarding?~~ ~~b. Generalized forwarding?~~

~~**Ans.** Longest prefix matching; Flow priorities~~

Q61. [3 marks] Suppose two packets arrive to two different input ports of a router at exactly the same time. Also suppose there are no other packets anywhere in the router.

a. Suppose the two packets are to be forwarded to two different output ports. Is it possible to forward the two packets through the switch fabric at the same time when the fabric uses a shared bus?
b. Suppose the two packets are to be forwarded to two different output ports. Is it possible to forward the two packets through the switch fabric at the same time when the fabric uses switching via memory?
c. Suppose the two packets are to be forwarded to the same output port. Is it possible to forward the two packets through the switch fabric at the same time when the fabric uses a crossbar?

Ans. No, No, No

Q62. [3 marks] Consider the two ways in which communication occurs between a managing entity and a managed device: request-response mode and trapping. What are the pros and cons of these two approaches, in terms of (1) overhead, (2) notification time when exceptional events occur, and (3) robustness with respect to lost messages between the managing entity and the device?

Ans.

a. Overhead: request-response > trapping

Request response mode will generally have more overhead (measured in terms of the number of messages exchanged) for several reasons. First, each piece of information received by the manager requires two messages: the poll and the response. Trapping generates only a single message to the sender. If the manager really only wants to be notified when a condition occurs, polling has more overhead, since many of the polling messages may indicate that the waited-for condition has not yet occurred.

b. Notification time: request-response > trapping

Trapping generates a message only when the condition occurs. Trapping will also immediately notify the manager when an event occurs. With polling, the manager needs will need to wait for half a polling cycle (on average) between when the event occurs, and the manager discovers (via its poll message) that the event has occurred.

c. Robustness: request-response < trapping

If a trap message is lost, the managed device will not send another copy. If a poll message, or its response, is lost the manager would know there has been a lost message (since the reply never arrives). Hence the manager could repoll, if needed.

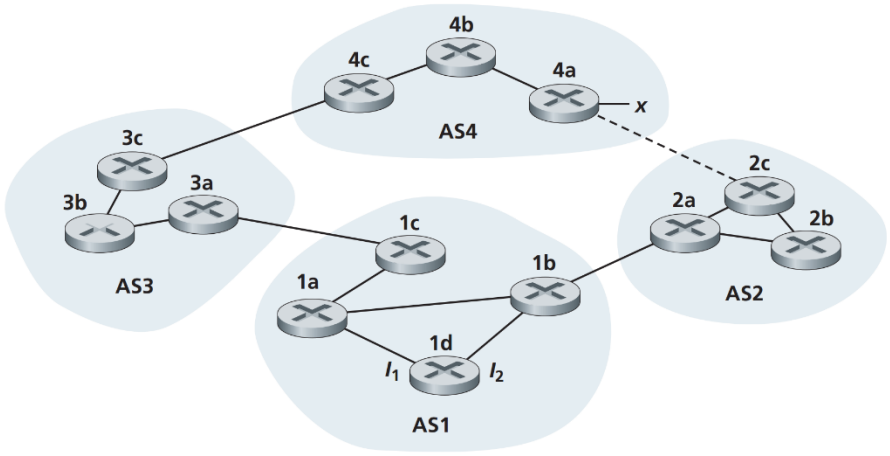
Q63. [4 marks] Suppose an ISP owns the block of addresses of the form 128.119.40.64/26. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. What are the prefixes (of form a.b.c.d/x) for the four subnets?

Ans. 128.119.40.64/28, 128.119.40.80/28, 128.119.40.96/28, 128.119.40.112/28

Q64. [7 marks] Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.

a. Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP, or iBGP?
b. Router 3a learns about x from which routing protocol: OSPF, RIP, eBGP, or iBGP?
c. Router 1c learns about x from which routing protocol: OSPF, RIP, eBGP, or iBGP?
d. Router 1d learns about x from which routing protocol: OSPF, RIP, eBGP, or iBGP?

Once router 1d learns about x it will put an entry (x, I) in its forwarding table.



e. Will I be equal to I1 or I2 for this entry? Explain why in one sentence.
f. Now suppose that there is a physical link between AS2 and AS4, shown by the dotted line. Suppose router 1d learns that x is accessible via AS2 as well as via AS3. Will I be set to I1 or I2? Explain why in one sentence.
g. Now suppose there is another AS, called AS5, which lies on the path between AS2 and AS4 (not shown in diagram). Suppose router 1d learns that x is accessible via AS2 AS5 AS4 as well as via AS3 AS4. Will I be set to I1 or I2? Explain why in one sentence.

Ans.

a. eBGP
b. iBGP
c. eBGP
d. iBGP
e. I1, because this interface begins the least cost path from 1d towards the gateway router 1c.
f. I2. Both routes have equal AS-PATH length but I2 begins the path that has the closest NEXT-HOP router.
g. I1. I1 begins the path that has the shortest AS-PATH.