CSC175 Data Communications & Networking Spring 2026 Final Exam

Student Name:__________________ ID： __________________

Total pts	

Note: For Q2-Q9, **it is recommended that you provide a short explanation for each answer key.** If your answer is correct, you will get the full point without the explanations. But in case your answer is incorrect, the explanations may earn you some partial credit.

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
/10	/15	/10	/16	/10	/14	/10	/8	/7

Q1 (10 pts) Multiple-choice questions: enter your answer keys here:

1	2	3	4	5	6	7	8	9	10

For the following multiple-choice questions, each question has exactly one correct answer key. If multiple choices are correct, choose the option “All of the above”. Fill in the answer keys in the table above. **(Answer keys written in the question area will not be counted.)**

1. What is the main purpose of TTL in IPv4?
A. To indicate the packet priority.
B. To identify all fragments of one packet.
C. To prevent indefinite forwarding loops by limiting hop count.
D. To measure propagation delay.

2. How does the sender respond when a packet or its acknowledgment is dropped?
A. It waits forever.
B. It sends a negative acknowledgment.
C. It uses a timer and retransmits when the timer expires.
D. It changes the port number.

3. What is the congestion window (cwnd)?
A. A receiver-side field that chooses the port number.
B. A sender-side output of the congestion-control algorithm that limits sending rate.
C. A checksum used only on duplicate acks.
D. A fixed constant equal to the MSS.

4. Suppose a TCP sender transmits a segment with sequence number j carrying B bytes. If all prior data has been received in order, what ACK value will the receiver send after correctly receiving this segment?
A. j
B. j + B − 1
C. j + B
D. j + 2B

5. In slow start, what rate-adjustment behavior causes the window to grow exponentially?
A. Adding a fixed number of packets to CWND each RTT
B. Halving CWND on every ACK
C. Doubling CWND every RTT by adding one packet per ACK in that RTT
D. Keeping CWND constant and only adjusting the timeout

6. What role does SSTHRESH play in TCP congestion control?
A. It stores the maximum allowed RTT
B. It records the last observed loss rate
C. It remembers a "safe" window size where slow start should stop and AIMD should begin
D. It indicates the number of duplicate ACKs seen so far

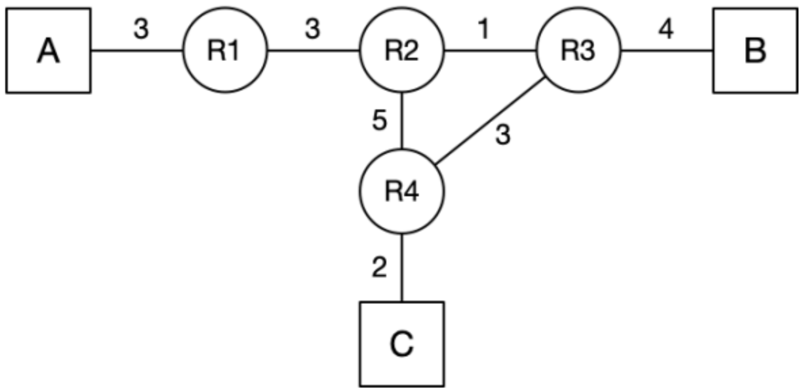
7. What key idea underlies fast recovery in TCP Reno/New Reno?
A. Use ECN bits to avoid all packet loss
B. Grant temporary "credit" for each duplicate ACK to keep packets in flight
C. Reset CWND to 1 packet after every loss
D. Move congestion control into routers instead of hosts

8. What is a DNS name server?
A. A host that only caches HTTP responses
B. A server responsible for answering DNS requests for some set of domains
C. Any router participating in BGP
D. A server that assigns IP addresses using DHCP

9. In an active attack, where an attacker captures a valid message and later retransmits it to produce an unauthorized effect, the attack is called:
A. Masquerade
B. Replay
C. Eavesdropping
D. Traffic analysis

10. Which protocol is specifically used for establishing a shared secret key over an insecure channel, rather than directly encrypting data?
A. RSA
B. Diffie–Hellman key exchange
C. AES
D. DES

Q2. (15 pts) Distance Vector (count-to-infinity)
Assume the following:
Routers run a **distance-vector** algorithm with no poisoned reverse or route poisoning, though **split horizon** is enabled. The routing algorithm uses incremental and triggered updates: when a router's table changes, it immediately advertises only the routes that changed. Routers send periodic routing updates **every 2 seconds** starting at t=0 s. Routing table entries expire after **TTL = 6** seconds of receiving no routing updates. Link costs equal propagation delay in seconds.



(a) (2 pts) Fill in the routing table of **R4** after all routes converge.

To	Next-hop Router	Cost
A		
B		
C	Direct	2

(b) (3 pts) Assume that all router-to-host direct links are initialized at time t = 0. How long will it take for R4's routing table to reach its converged state, starting from time t = 0?

(c) (4 pts) Assume that at time t: All routers have converged. All routers send their periodic advertisements at time t-4, t-2, t…. Assume at time t+1, R1 crashes. How many seconds after t will R2’s routing table reflect the failure of R1?

(d) (6 pts) Regardless of your answer to the previous subpart, assume R2’s routing table reflected the failure of R1 at time t'. Assume t' is the time at which all routers send periodic advertisements as well. Fill out the routing table at R2 and R3 at time t'+3. All rows at the table should be filled. Ignore all triggered updates that might have happened prior to t', but do consider any periodic updates that have happened (for example at time t'-2). (Recall that **split horizon** is enabled.)

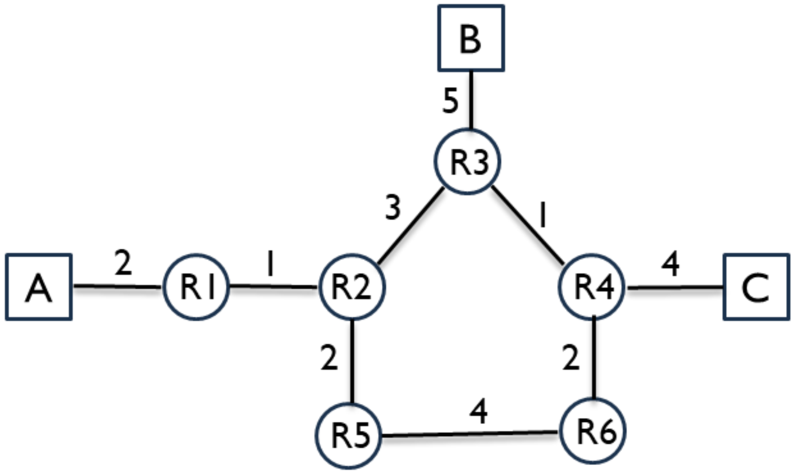
Routing table of **R2:**

To	Next-hop Router	Cost
A		
B		
C		

Routing table of **R3:**

To	Next-hop Router	Cost
A		
B	Direct	4
C		

Q3. (10 pts) Link-State (link failure)
Consider a network with three hosts (A, B, C) and routers R1–R6. Routers are running **link state** algorithm. Link costs equal propagation delay in seconds.



(a) (2 pts) The link R3–R4 fails. R3 and R4 have recomputed their routes but have not yet sent updates. Suppose R3 and R4 never send any updates. What route does a packet from A to C take?

(b) (3 pts) The link R5–R6 fails instead of R3–R4. R5 and R6 have recomputed their routes but have not yet sent updates. Suppose R5 and R6 never send any updates. What route does a packet from A to C take?

(c) (5 pts) At t = 0 a packet from A arrives at R1, destined for C. At t = 3.5 s the link R3–R4 goes down. R3 and R4 recognize and recompute instantly; routing updates propagate at the link prop delay. List the packet path and complete a timing table for every packet arrival and LSA arrival until the packet reaches C (or is detected as undeliverable).

t (s)	Event
0	Packet arrives at R1

Q4. (16 pts) Longest Prefix Matching

A router has 4 ports, with routing table shown below. The routes are written using canonical CIDR notation. Use these rules in order: longest prefix match, then lowest cost, then smallest port number. If no prefix matches, use the **default route on port 1**. Given the routing table below, for each destination IP address, determine **the output port** to forward it, and **the routing table entry** used to make that routing decision, and with a brief explanation.

Routing table

Port	Destination	Cost
1	1.0.0.0/8	10
1	2.1.0.0/16	15
1	2.2.192.0/20	12
1	4.0.0.0/8	10
1	2.2.0.0/17	15
2	1.1.0.0/16	8
2	2.2.128.0/17	14

2	4.0.0.0/8	8
3	3.0.0.0/8	10
3	2.2.192.0/20	13
3	1.0.10.0/24	8
4	3.4.0.0/16	11
4	1.1.0.0/16	8
4	2.2.0.0/17	14

You can find some useful binary conversions in the table below.

Decimal	**Binary**
192	11000000
128	10000000
96	01100000
208	11010000
64	01000000
32	00100000

(a) (2 pts) A packet with destination 3.4.0.1

(b) (2 pts) A packet with destination 4.0.0.1

(c) (2 pts) A packet with destination 2.2.208.1

(d) (2 pts) A packet with destination 2.3.0.10

(e) (2 pts) A packet with destination 2.2.204.13

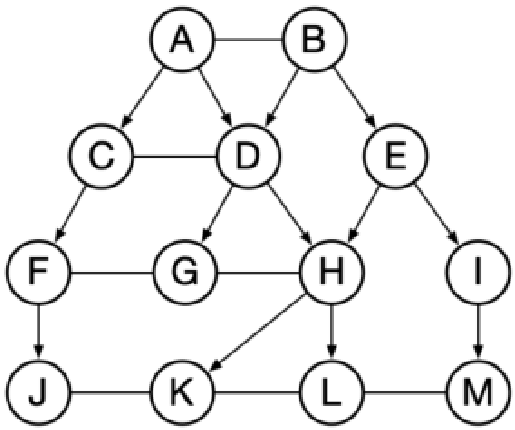
(f) (2 pts) A packet with destination 1.1.21.7

(g) (2 pts) A packet with destination 2.2.96.22

(h) (2 pts) A packet with destination 1.0.10.5

Q5. (10 pts) Inter-Domain Routing under Gao-Rexford

Consider the AS graph below, where each AS follows the Gao-Rexford import and export policies. Provider to Customer relationship is denoted by arrows; peer to peer relationship is denoted by horizontal lines with dots. (Hint: Every intermediate AS on a legal path must have at least one customer neighbor along that path. Valid AS paths should be valley-free: traffic goes up provider links zero or more times, may cross at most one peer link, and then goes down customer links zero or more times.)



(a) (6 pts) Determine the path (if any) between the following ASes. If there is no path possible, write "None".

(1) J to M

(2) L to F

(3) E to F

(b) (2 pts) When AS D sends BGP advertisements to AS C, which destination ASes can appear in those advertisements?

(c) (2 pts) The link between CD fails, what is the path from J to L?

Q6. (14 pts) TCP Sequence Diagram (fill in seq number)

Consider the TCP sequence diagram with sequence numbers in Bytes. Assume each message segment size is 10 bytes; send window (cwnd) size = 20 bytes. (Assume there is no congestion control, so the send window (cwnd) size is constant.) Upon detecting a packet loss, TCP retransmits the leftmost unacknowledged segment. Give the sequence numbers for each message and ACK.

(a) Timeout scenario

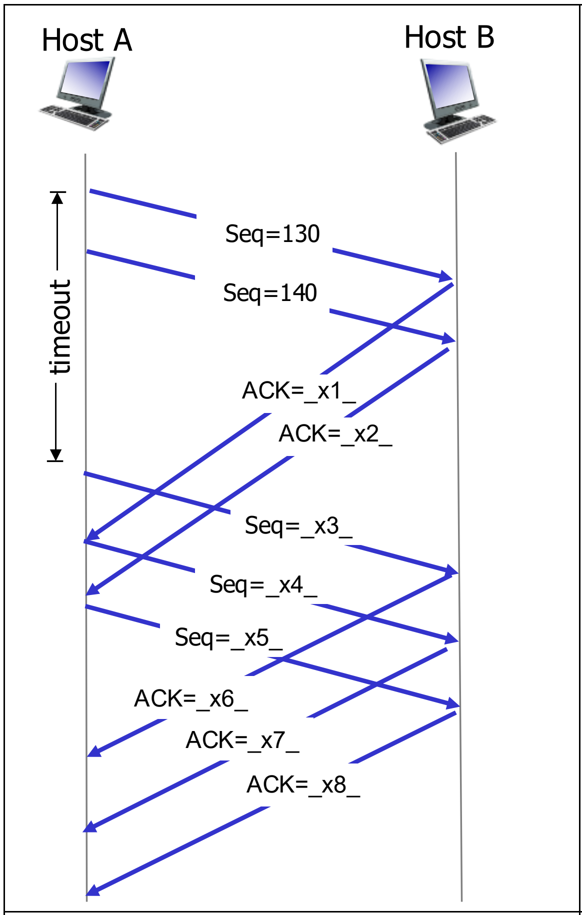
x1 = __________, x2 = __________, x3 = __________, x4 = __________,

x5 = __________, x6 = __________, x7 = __________, x8 = __________.

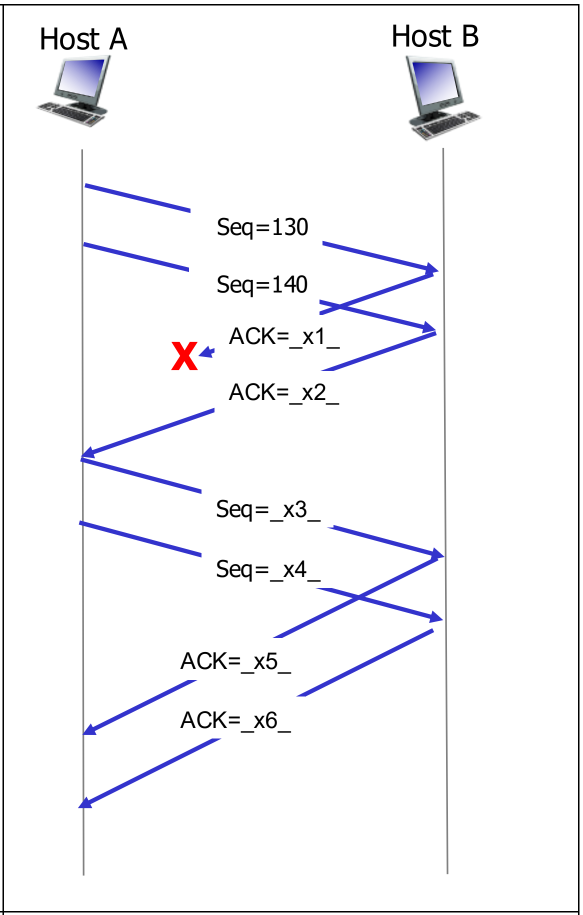
(b) Ack loss scenario

x1 = __________, x2 = __________, x3 = __________, x4 = __________,

x5 = __________, x6 = __________.



(a) Timeout scenario



(b) Ack loss scenario

Q7. (10 pts)TCP Congestion Control (CWND vs time)
Consider the figure that plots the evolution of TCP's congestion window at the beginning of each time unit (where the unit of time is equal to number of RTTs). The (x, y) coordinates of key points are marked in the figure. TCP sends a "flight" of packets of size cwnd at the beginning of each time unit. The initial value of cwnd is 1. Assume: **TCP new Reno** (slow start + congestion avoidance + fast recovery. Lecture slide attached below for your reference). Loss detected via triple duplicate ACK or timeout. Assume no gap between detecting a packet loss and sending out the next packet.

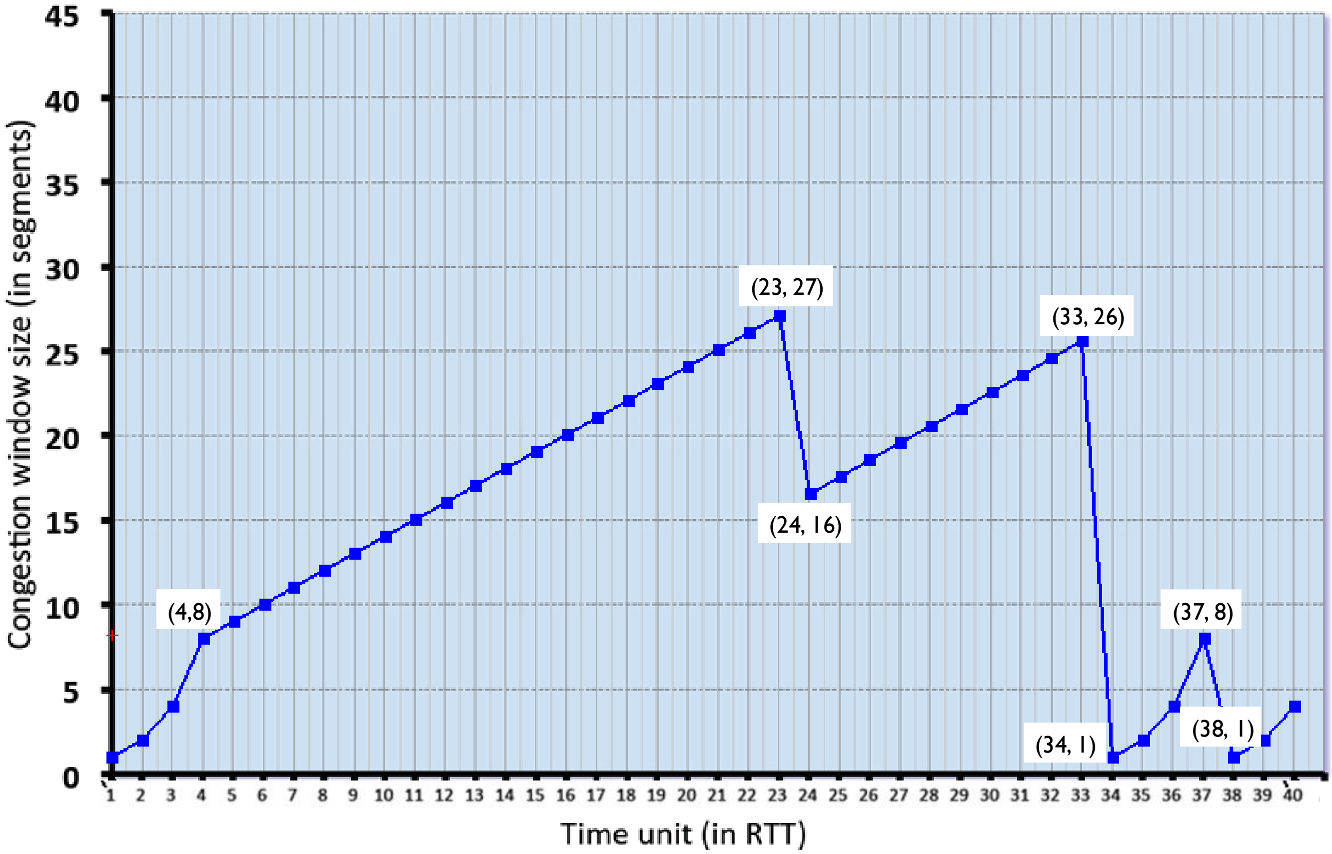
Fast Recovery: Implementation

Conceptually: When a duplicate ack arrives, *artificially extend* the window to let the sender send one more packet.

Implementation:

- When we receive 3 duplicate acks:
  - *SSTHRESH* ← *CWND*/2
  - *CWND* = *CWND*/2 + 3 *(artificially extend for the 3 duplicate acks)*
- While in fast recovery mode, when we receive a duplicate ack:
  - *CWND* = *CWND* + 1 *(artificially extend for each duplicate ack)*
- Exit fast recovery when we receive a new, non-duplicate ack:
  - *CWND* = *SSTHRESH* *(back to 0.5 × rate when the loss happened)*

Note: if cwnd is an odd number, then take the floor (cwnd = $\lfloor \frac{cwnd}{2} \rfloor$).



Q7.1 Identify the RTT intervals where slow start is operating.

Q7.2 Identify the RTT intervals where congestion avoidance is operating.

Q7.3 At which RTT does the first loss event occur? What type is it?

Q7.4 At which RTT does the second loss event occur? What type is it?

Q7.5 What is the initial ssthresh (before time 1)?

Q7.6 What are the values of ssthresh and cwnd immediately after the first loss?

Q7.7 What are the values of ssthresh and cwnd immediately after the second loss?

Q7.8 What is the maximum cwnd reached before each loss event?

Q7.9 Based on the graph, does TCP return to slow start after the first loss event?

Q7.10 How many segments are sent during RTTs 1–6?

Q8. (8 pts) CBC Block Cipher

Consider the 3-bit block cipher in the Table below

Plain	000	001	010	011	100	101	110	111
Cipher	111	110	101	100	011	010	000	001

Suppose the plaintext is 010111010.

(a) (2 pts) Without Cipher Block Chaining (CBC), what is the ciphertext? Show the calculation process.

(b) (6 pts) With CBC and IV = 111, what is the ciphertext? Show the calculation process.

Q9. (7 pts) Diffie-Hellman

Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob agree on a prime $p = 11$ and a generator $g = 2$.

- Alice chooses her secret number (private exponent) as $a = 3$.
- Bob chooses his secret number (private exponent) as $b = 4$.

Show the step-by-step calculation process:

(a) (2 pts) The value Alice sends to Bob.

(b) (2 pts) The value Bob sends to Alice.

(c) (3 pts) The final shared secret computed by both sides.