CSS334: Computer Network and Internetworking

Midterm Mock Exam

curated by The Peanuts

Name . . . . . ID . . . . . Section . . . . . Seat No . . . . . .

Conditions: Semi-closed Book

Directions:

1. This exam has 16 pages. If yours has fewer, your copy experienced packet loss. There is no retransmission. No timeout will save you.
2. Write your name and ID at the top of every page.
3. Show all steps in Problem Solving.
4. Do not communicate with neighboring hosts during the exam.
5. Manage your time. This exam is 2 hours. That is your RTT budget. If you are still on Question 1 at the 90-minute mark, your congestion window is critically low, consider fast retransmit.

For solution, ***click here****.*

Part I: Multiple Choice

Choose the best answer for each question. (2 points each)

1. Which statement about TCP is NOT correct?

a) TCP provides reliable, in-order byte stream delivery.

b) TCP guarantees minimum bandwidth and end-to-end delay for applications.

c) TCP uses a 3-way handshake to establish a connection before data transfer.

d) TCP performs both flow control (via `rwnd`) and congestion control (via `cwnd`).

2. According to the TCP protocol, which statement about demultiplexing is correct?

a) TCP uses only the destination port number to identify the receiving socket.

b) TCP uses a 4-tuple (source IP, source port, destination IP, destination port) to identify each unique socket.

c) Two TCP connections from different clients to the same server port always share the same socket.

d) TCP demultiplexing works identically to UDP demultiplexing.

3. Regarding the TCP 3-way handshake, which statement is NOT correct?

a) The client sends a SYN segment containing its chosen initial sequence number x.

b) The server replies with a SYN-ACK segment containing its initial sequence number y and `ACKnum = x+1`.

c) The TCP connection is fully established as soon as the server sends the SYN-ACK, before receiving the third ACK. & stay at SYN-received

d) The third message (ACK from client) may carry client-to-server data inside the same segment.

4. Which statement about the UDP checksum is correct?

a) The checksum provides guaranteed error correction; the receiver can repair corrupted bits.

b) The checksum is computed as the one's complement of the sum of all 16-bit words in the segment (with wraparound carry).

c) If the receiver detects a checksum mismatch, UDP automatically retransmits the segment.

d) The UDP checksum covers only the application data payload, not the UDP header.

5. Which statement about HTTP is NOT correct?

a) HTTP is a stateless protocol; the server maintains no information about past client requests.

b) HTTP 1.1 introduced persistent connections, reducing the RTT overhead of HTTP 1.0.

c) HTTP/2 fully eliminates Head-of-Line (HOL) blocking by opening a separate TCP connection per object.

d) Non-persistent HTTP (1.0) requires 2 RTT + file transmission time per object retrieved.

6. According to the Go-Back-N (GBN) protocol, which statement is correct?

a) The receiver buffers correctly received out-of-order packets and acknowledges them individually.

b) The receiver sends an ACK only for the highest in-order packet received; out-of-order packets are discarded.

c) Upon timeout of packet n, only packet n is retransmitted; packets $n{+}1, n{+}2, \ldots$ are not.

d) GBN and Selective Repeat have the same retransmission behavior on packet loss.

7. Which statement about TCP Reno's behavior on detecting 3 duplicate ACKs is <u>NOT</u> correct?

a) TCP Reno retransmits the missing segment immediately, without waiting for a retransmission timeout.

b) TCP Reno sets ssthresh = cwnd/2 and sets cwnd = ssthresh, then grows linearly.

c) Receiving 3 duplicate ACKs indicates that some segments after the lost one were successfully received.

d) TCP Reno resets cwnd = 1 MSS and restarts slow start after 3 duplicate ACKs.

8. Which statement correctly describes the relationship between TCP flow control and TCP congestion control?

a) Flow control uses `cwnd`; congestion control uses `rwnd`.

b) Flow control prevents the sender from overwhelming the receiver's buffer; congestion control prevents the sender from overwhelming the network.

c) Flow control and congestion control both adjust the sender's window using the same `rwnd` field.

d) Congestion control is performed exclusively by routers; the end hosts have no role in it.

9. Which statement about DNS is NOT correct?

a) DNS uses a three-level hierarchy: root servers, Top-Level Domain (TLD) servers, and authoritative servers.

b) DNS resolution can use either recursive queries (resolver does the work) or iterative queries (client does the work).

c) DNS resource records are cached indefinitely by local resolvers to minimize repeated queries.

d) DNS can map a single domain name to multiple IP addresses, enabling load distribution across servers.

10. Which statement about port number ranges is correct?

a) Well-known ports range from 0 to 1,023 and are reserved for common, standardized services.

b) Registered ports range from 1,024 to 65,535, covering both registered and dynamic/ephemeral ports.

c) A single IP address cannot simultaneously run an HTTP server on TCP port 80 and another application on UDP port 80.

d) Dynamic (ephemeral) ports are manually assigned by the application developer at compile time.

Part II: Fill in the Blank

Fill in each blank with the most appropriate keyword.

1. DNS is a protocol that translates human-readable domain names into IP addresses; it is distributed hierarchically and primarily operates over UDP on port **53**.

2. HTTP is a protocol used by web browsers to request and retrieve web pages from servers; it is stateless and operates over TCP on port **80**.

3. SMTP is a protocol used to transfer email messages between mail servers; it operates over TCP on port **25** and is responsible for sending, not retrieving, mail.

4. UDP is a transport-layer protocol that provides connectionless, best-effort delivery with no handshaking, no congestion control, and minimal header overhead (just 8 bytes). It is commonly used by DNS, SNMP, and streaming applications.

5. In TCP's flow control mechanism, the rwnd field in the TCP segment header is advertised by the receiver to inform the sender of the remaining free buffer space available, preventing buffer overflow.

6. A TCP socket is uniquely identified by a 4-tuple consisting of four values: source IP address, source port number, destination IP address, and destination port number.

7. Selective repeat is a pipelined reliable data transfer protocol in which the receiver buffers correctly received out-of-order packets and acknowledges each one individually, so that only the specific lost packet needs to be retransmitted.

8. When a TCP sender receives **three duplicate ACKs** for the same sequence number, it immediately retransmits the missing segment without waiting for a timeout. This mechanism is called fast retransmit.

9. In TCP's congestion control, the slow start phase ends and transitions to congestion avoidance (linear increase) when the congestion window `cwnd` reaches the ssthresh threshold value. On a loss event, this threshold is set to half of the current `cwnd`.

10. IMAP is an email retrieval protocol that allows users to manage messages stored on a remote mail server from multiple devices, keeping messages synchronized on the server; it operates over TCP on port **143**.

Part III: Short Answer

Answer each question concisely. Show key reasoning where applicable. (6 points each)

Question 1

Explain the difference between **non-persistent HTTP (HTTP 1.0)** and **persistent HTTP (HTTP 1.1)**.

(a) State the response time formula for non-persistent HTTP when retrieving a single object, and briefly explain what each term represents.

2RTT + file transmission time

(b) A web page contains 1 base HTML file and 8 referenced images, all on the same server. Using **non-persistent HTTP**, how many TCP connections are required and what is the total response time in terms of RTT?

There are 9 objects in total (1 base HTML file + 8 images).

Therefore:

- Number of TCP connections = 9
- Total response time =

9 x (2RTT + transmission time)

Question 2

Describe the **TCP 3-way handshake** used to establish a connection between a client and a server.

(a) List the three steps, specifying which flag bits are set and what sequence/ACK numbers are exchanged in each step. Let the client's initial sequence number be x and the server's initial sequence number be y.

Step 1:
Client sends a segment with SYN = 1 and sequence number = x.

Step 2:
Server replies with SYN = 1, ACK = 1,
sequence number = y, and acknowledgment number = x + 1.

Step 3:
Client sends ACK = 1 with
sequence number = x + 1 and acknowledgment number = y + 1.

(b) What is a **SYN flood attack**? Explain briefly why the 3-way handshake creates a vulnerability that this attack exploits.

A SYN flood attack is a denial-of-service attack in which an attacker sends many SYN segments but never completes the handshake.

This creates many half-open connections on the server, consuming its resources and preventing legitimate clients from connecting.

Question 3

Compare **Go-Back-N (GBN)** and **Selective Repeat (SR)** by answering the following:

(a) Does the receiver buffer out-of-order packets in GBN? In SR? What is the consequence of each design choice?

- In Go-Back-N (GBN), the receiver does not buffer out-of-order packets.
  Out-of-order packets are discarded.
- In Selective Repeat (SR), the receiver buffers correctly received out-of-order packets.
- As a result, GBN may retransmit multiple packets after a loss, while SR retransmits only the specific lost packet.

(b) A GBN sender has window size $N = 4$ and has sent packets 0, 1, 2, 3. Packet 1 is lost. Packets 2 and 3 arrive correctly at the receiver. Describe exactly what the receiver does with packets 2 and 3, and what the sender must retransmit after the timeout.

- When the receiver receives packets 2 and 3, it discards them because packet 1 is missing.
  It repeatedly sends ACK = 1 (cumulative acknowledgment).
- After timeout, the sender retransmits packets 1, 2, and 3.

(c) What type of ACK does each protocol use: cumulative or individual? Explain the difference in one sentence each.

- GBN uses cumulative ACKs.
  A cumulative ACK acknowledges the highest in-order packet received.
- SR uses individual ACKs.
  Each correctly received packet is acknowledged separately.

Question 4

TCP uses two distinct window-based mechanisms to control the sender's transmission rate.

(a) Explain **flow control**: what problem it solves, who controls whom, and which field in the TCP header implements it.

- Flow control prevents the sender from overwhelming the receiver's buffer.
- The receiver controls the sender by advertising the available buffer space using the **rwnd (receiver window)** field in the TCP header.

(b) Explain **congestion control**: what problem it solves and which variable TCP dynamically adjusts to respond to congestion.

- Congestion control prevents the sender from overwhelming the network.
- TCP dynamically adjusts the congestion window (**cwnd**) to control the sending rate.

(c) Write the inequality that governs the maximum amount of unacknowledged ("in-flight") data a TCP sender may have outstanding at any time, incorporating both `rwnd` and `cwnd`.

Last Byte Sent - Last Byte Ack < min(cwnd , rwnd)

Question 5

A user on a laptop types `www.siit.tu.ac.th` into a browser for the first time.

(a) Briefly describe the role of each of the following in the DNS resolution process: **local resolver**, **root DNS server**, **TLD DNS server**, and **authoritative DNS server**.

- The local resolver receives the query from the client and performs the resolution process.
- The root DNS server provides the address of the appropriate TLD server.
- The TLD DNS server provides the address of the authoritative server.
- The authoritative DNS server returns the final IP address of the domain.

(b) What is the difference between a **recursive** DNS query and an **iterative** DNS query? Describe which entity performs the lookups in each case.

- In a recursive query, the resolver performs all the lookups on behalf of the client.
- In an iterative query, the client (or resolver) contacts each DNS server step by step.

(c) Why does DNS primarily use **UDP** rather than TCP? Under what circumstance might DNS fall back to TCP?

- DNS primarily uses UDP because it is faster and has lower overhead.
- DNS uses TCP when the response size exceeds the UDP limit or during zone transfers.

Part IV: Problem Solving

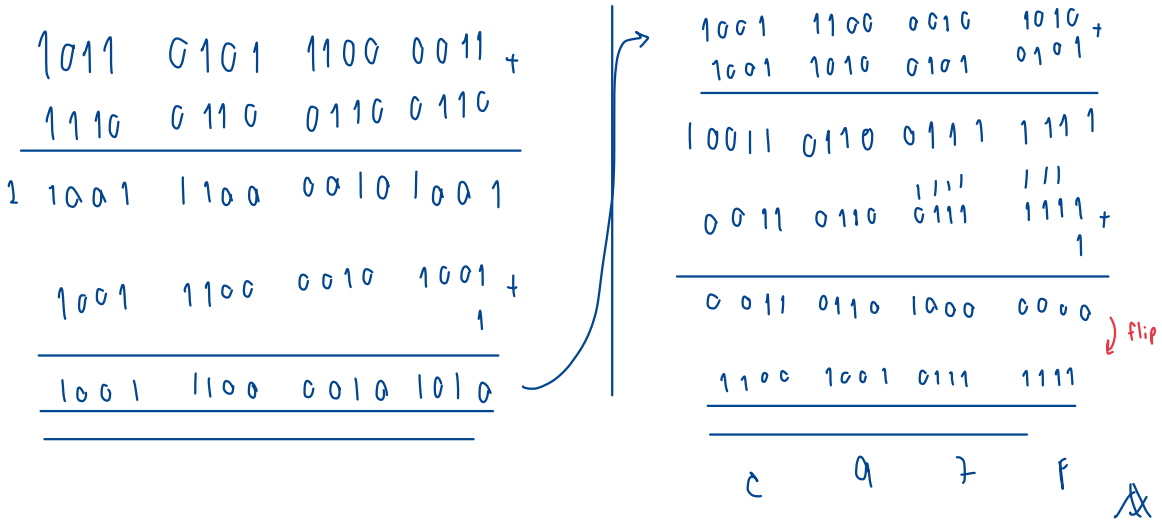
Show ALL steps. Partial credit is given. (15 points each)

Problem 1

A UDP sender transmits a segment whose payload consists of the following three 16-bit words:

Word 1:	1011 0101 1100 0011
Word 2:	1110 0110 0110 0110
Word 3:	1001 1010 0101 0101

(10 pts) Compute the **Internet checksum** that the sender places in the UDP header. Show all intermediate binary arithmetic clearly. Express your final answer in both **binary** and **hexadecimal**.



(5 pts) The receiver recomputes the checksum over all four 16-bit words (Word 1, Word 2, Word 3, and the received checksum field). State the expected result and explain in one sentence what it means when the receiver obtains this value.

expect result is 1111 1111 1111 1111

This means no error is detected in transmission.

Problem 2

Host A establishes a TCP connection with Host B. Host A's initial sequence number (ISN) is **100**. Host A then sends three consecutive TCP data segments to Host B:

↳ byte number of first byte

Segment	Data Size
Segment 1	20 bytes
Segment 2	30 bytes
Segment 3	15 bytes

Segment 2 is lost (never arrives at Host B). Segments 1 and 3 arrive at Host B successfully. At the time of the loss event, Host A's congestion window is `cwnd` = 8 MSS.

(a) **(3 pts)** State the **sequence number** of the first byte in each of the three segments (Segment 1, Segment 2, Segment 3).

Seg 1 first byte : 100 } 20
Seg 2 : 120 } 30
Seg 3 : 150

Seg 1 first byte : 100
Seg 1 last byte : 119
next byte : 120 → Ack
Seg 3 last byte : 149
next byte : 150 → Ack

(b) **(3 pts)** What **ACK number** does Host B send back to Host A after successfully receiving **Segment 1**? What does this ACK number indicate?

ACK = 120, This indicates that all bytes up to 119 have been received successfully and the receiver expects byte 120 next.

(c) **(3 pts)** Host B receives Segment 3 (out of order, since Segment 2 was lost). What **ACK number** does Host B send in response to Segment 3, and why?

ACK 120 , This is a duplicate ACK because Segment 2 is missing.

(d) **(3 pts)** Host A receives **three duplicate ACKs** for sequence number 120. Assuming **TCP Reno**, describe the **fast retransmit** action taken, and state the new values of `cwnd` and `ssthresh` after the event.

- The sender performs fast retransmit of Segment 2.
- ssthresh = cwnd / 2 = 8 / 2 = 4 MSS
- cwnd = ssthresh + 3 MSS = 7 MSS

The sender enters fast recovery.

(e) **(3 pts)** If Host A were using **TCP Tahoe** instead of TCP Reno, how would its response to the same 3 duplicate ACKs differ? State the new `cwnd`, `ssthresh`, and the phase TCP enters.

- ssthresh = 4 MSS
- cwnd = 1 MSS
- TCP enters slow start phase.

Tahoe does not implement fast recovery.