CS 118 – Fall 2002
Sample Midterm #1 Solutions

You may use a single 8 ½ x 11 sheet of paper, front and back, with any notes you like. You may also use a calculator.

1. (7) True or False:

(a) Error control for reliable transfer is implemented only at the link layer.
FALSE – Implemented at many layers

(b) In a circuit switched network, after setting up an end-to-end circuit, the transfer time of a file is deterministic, not random.
TRUE – no congestion occurs in circuit switched networks

(c) UDP is an unreliable datagram protocol because it does not check packets for errors upon arrival, whereas TCP does verify the checksum on incoming packets.
FALSE – UDP does calculate checksums and check for corrupt packets

(d) Reliable data transfer can not be achieved if an unreliable transport protocol such as UDP is used.
FALSE – RDT may be implemented at the application layer

(e) Congestion control is not needed over circuit switched networks.
TRUE – no congestion since circuits are reserved

(f) The number of entries in the root DNS servers grows linearly with the number of end-systems (hosts) using the Internet.
FALSE – The DNS database is stored hierarchically, so not every host has an entry at the RNS's.

(g) Sockets provide the interface between the transport layer and the network layer.
FALSE – Sockets provide the interface between the Application Layer and the Transport Layer

2. (3) For each of the following scenarios, indicate (with an X in the appropriate column) whether it favors packet switching, circuit switching, or neither.

Scenario:	Favors Packet Switching	Favors Circuit Switching	Neither
i. Bursty Data	**X**		
ii. Narrow bandwidth relative to user demand for transferring data	**X**		**X**
iii. Delay Sensitive Applications		**X**	

(for ii. Both answers are acceptable)

3. (5) List and briefly describe all of the application and transport layer protocols used to download a webpage.

Application Layer – **HTTP for downloading web content**
DNS for obtaining IP address of server

Transport Layer – **TCP for carrying HTTP requests/responses**
UDP for carrying DNS requests/responses

4. (15) Compare the delay in sending an *x*-bit message over a *k*-hop path (i.e. *k-1* intermediate switches/routers) in a circuit switched network and in a packet switched network. The circuit setup time is *s* seconds. The propagation delay is *d* seconds per hop, the packet size is *p* bits, and the data rate for all links is *b* bps. Under what conditions does the packet switched network have a lower delay?

Answer:
Total delay of packet switching is calculated in terms of the last packet. At time $\frac{x}{b}$ it is sent over the first hop and after $(k-1)\frac{p}{b}$ transmission delay over the $k-1$ routers plus kd propagation delay over the *k* hops it arrives at destination.

The total delay of packet switching is:

$$T_{packet} = \frac{x}{b} + (k-1)\frac{p}{b} + kd$$

The total delay of circuit switching is:

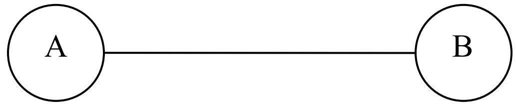
$$T_{circuit} = s + \frac{x}{b} + kd$$

Therefore, when $s > (k-1)\frac{p}{b}$, packet switching is better.

5. (10) If a DNS resolver at the host *windows.microsoft.com* tries to get the IP address of a non-existing host *nonexist.ucla.edu*, is the local DNS for the zone *microsoft.com* able to inform the DNS resolver that the given host is non-existing? Why or why not? Under what conditions can a given resolver get the IP address of existing host *cheetah.cs.ucla.edu* faster than to get the information about the above-mentioned non-existing host?

Answer:
The DNS server for *microsoft.com* cannot know that the host doesn't exist until the DNS server for *ucla.edu* is queried. For existing host *cheetah.cs.ucla.edu*, the IP address may already be in the local cache of the DNS server for *microsoft.com*. Thus there would be no need to query the DNS server for *ucla.edu*.

6. (30) Given two hosts, connected by a single link:



- The propagation delay of the link is *d* seconds
- The link bandwidth is *R* bps
- For each TCP segment, header size is always *h* bits, payload size is always *p* bits. If payload sent from application layer is less than *p* bits, padding bits will be added so that the payload will be exactly *p* bits.
- TCP window size is fixed at 50
- There is no error or loss in transmission
- The client **A** requests a webpage from **B**, which contains 10 embedded images. Each object is exactly *2p* bits in size – therefore each object can be sent in exactly 2 packets.
- **A** already holds the IP address for **B** in its local cache

(a) (2) Give an expression (including units) for the Transmission Delay T_{trans} for each packet, including headers. Also derive an expression for the round trip time RTT.

$$T_{trans} = \frac{p+h}{R} \text{ seconds}$$

$$RTT = 2d \text{ seconds}$$

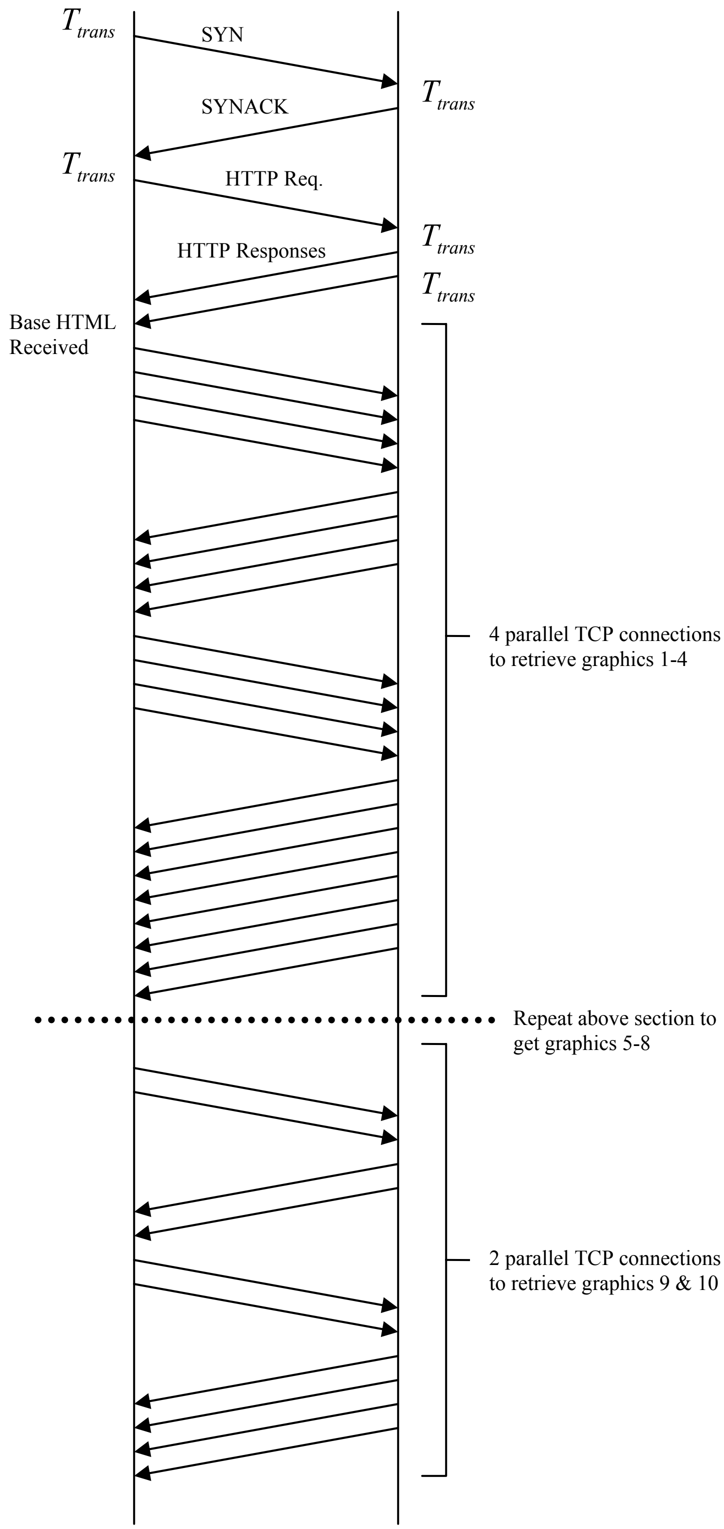
(b) What is the total delay required to view all the contents of the webpage in each of the following scenarios (give answers in terms of T_{trans} and RTT as derived in part a):

i. (7) Using non-persistent parallel HTTP connections (max. 4 parallel connections open at the same time, evenly sharing the bandwidth).

Answer:
(see diagram next page)

$$T_{base} = 5T_{trans} + 2RTT$$

$$T_{images} = 2(20T_{trans} + 2RTT) + (10T_{trans} + 2RTT)$$



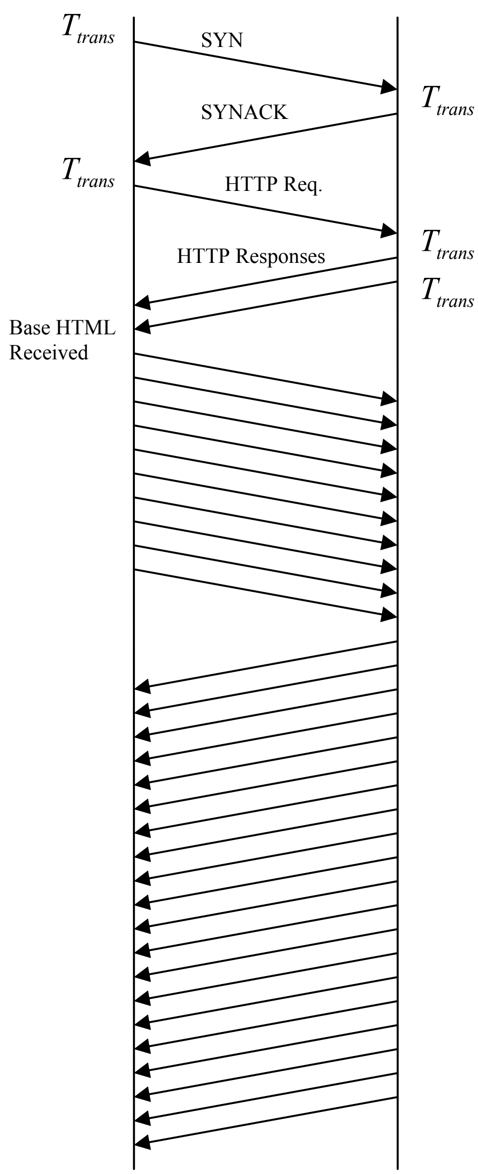
T_{trans}
SYN
T_{trans}
SYNACK
T_{trans}
HTTP Req.
T_{trans}
HTTP Responses
T_{trans}
Base HTML Received
4 parallel TCP connections to retrieve graphics 1-4
Repeat above section to get graphics 5-8
2 parallel TCP connections to retrieve graphics 9 & 10

ii. (7) Using persistent HTTP connections with pipelining. Assume that if there are back-to-back HTTP requests, the server will send responses after receiving all HTTP requests.

Answer:

$$T_{base} = 5T_{trans} + 2RTT$$

$$T_{images} = 30T_{trans} + RTT$$

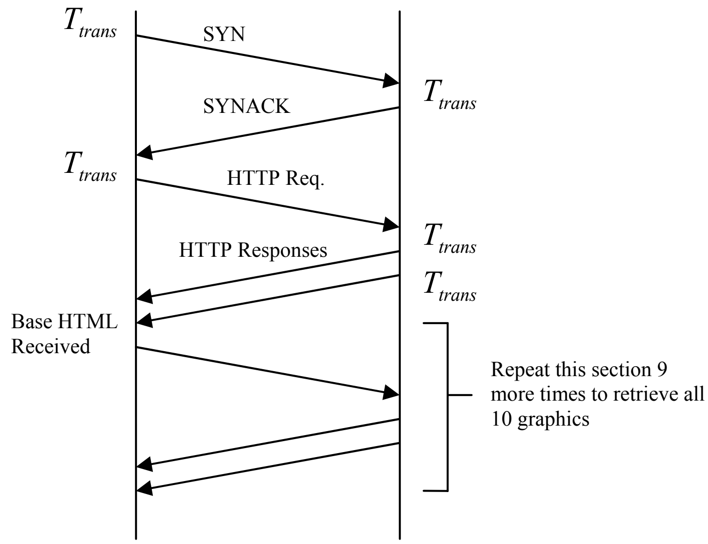


iii. (7) Using persistent HTTP connections without pipelining.

Answer:

$$T_{base} = 5T_{trans} + 2RTT$$

$$T_{images} = 10(3T_{trans} + RTT)$$

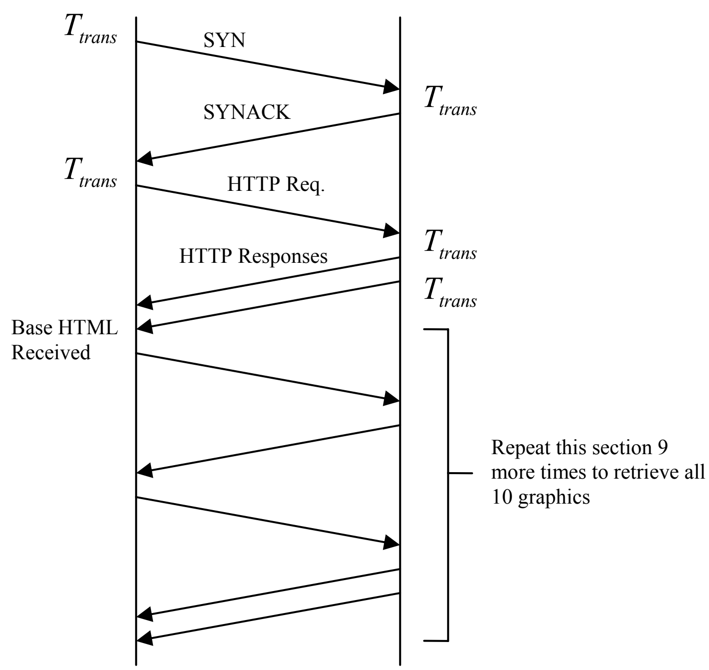


iv. (7) Using non-persistent and no parallel HTTP connections.

Answer:

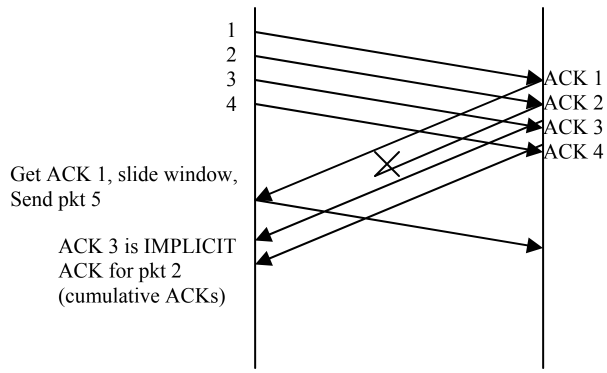
$$T_{base} = 5T_{trans} + 2RTT$$

$$T_{images} = 10(5T_{trans} + 2RTT)$$



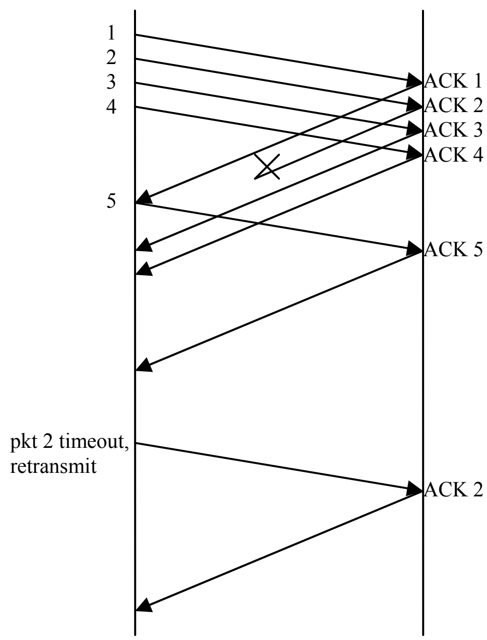
7. (10) Fill in the following charts

(a) (5) Assume a Go-Back-N protocol is used with a window size of 4 and that the ACK for packet 2 gets lost. Show the events until packet 2 is acknowledged at the sender side.



Answer:
Since GBN uses cumulative ACKs, when the ACK for packet 3 is received at the sender, it will be treated as an implicit ACK for packet 2 as well. In the meantime, when ACK 1 is received at the sender, the sender window will slide, and packet 5 will be sent.

(b) (5) Do the same for the Selective Repeat Protocol.



Answer:
SR does not use cumulative ACKs. When ACK 1 is received, the sender window slides, and pkt 5 is transmitted. pkts 3, 4, and 5 are received and buffered. When pkt 2 times out, it is retransmitted, ACK'd, and the window then slides past all ACK'd packets. Next packet to be transmitted will be pkt 6.

8. (10) A user at host A tries to fetch an HTML file from the HTTP server at host B. The HTTP server listens on its standard port 80. Show the following fields in the first three TCP segments exchanged to set up the connection: source port, destination port, sequence number, acknowledgement number, and flags SYN and ACK. Pick any appropriate initial sequence numbers.

NOTE: source port and sequence numbers are arbitrary (src. port must be >1024)

	TCP Source port	TCP Dest. Port	Seq. #	ACK #	SYN	ACK
A to B	**1025**	**80**	**50**	**–**	**1**	**0**
B to A	**80**	**1025**	**225**	**51**	**1**	**1**
A to B	**1025**	**80**	**51**	**226**	**0**	**1**

9. (10) Consider a TCP connection over a wide area network. Assume a malicious router drops every other segment on this connection (i.e. it drops 2, 4, 6, etc.). The TCP version is the Reno version supporting slow start, congestion avoidance, fast re-transmit, and fast recovery. Assume the receiver's advertised window is *awin=256*MSS*. Also, assume that there is plenty of bandwidth available on the path, so as to accommodate a TCP window *cwin = 64* without the malicious drop.

(a) What is the maximum window size achieved on this connection?

Answer:
W=2. The transmission of packet #2 causes timeout and slow start.

(b) Repeat (a) for the case in which the malicious router drops every eighth packet (i.e. 8, 16, 24, etc.) and no fast retransmit or fast recovery is used.

Answer:
W=8. The window grows to at most 8, then drops to 1 again, and so on.