EL5373
INTERNET ARCHITECTURE & PROTOCOLS

Final Examination

Name: ____

Student ID: ____

Instruction:

- *This exam booklet is a part of your submission. Please return it even if you have all the work shown on other answer sheets/book.*
- Remember to write your NAME and Student ID on this booklet as well as any separate answer sheets/book if you wish to attach.
- The Exam is Open Book. You can use your Text Book, printed lecture slides, notes or any other kind of printed/hand written material. Sharing of any material is not permitted.
- Calculators are allowed, but any kind of computers or communication devices are not.
- Be neat. Unreadable answers will not be graded.
- This booklet contains questions in seven Parts. All questions in each part need to be answered.
- *There may be more than one correct answer for the 10 multiple-choice problems in part I. You have to select all correct ones in each question.*

I. Circle ALL correct answers for the following 10 questions.

1. A host in an IP network can be identified by _____. Furthermore, an application running by this host can be identified by _____.

   a) a host MAC address, a well-known port number

   b) an IP address; a host name

   [✓ c)] an IP address; a port number

   d) a port number; an IP address

2. The value of Message Length in the header of a UDP Packet containing a 1496-byte payload is _____.

   a) 1488

   b) 1496

   c) 1516

   [✓ d)] none of the above

3. Consider a TCP connection between host A and host B. Suppose that the TCP segments traveling from host A to host B have source port number X and destination port number Y. Then source and destination port numbers for the segments traveling from host B to host A are

   a) Y+1 and X+1 respectively.

   b) Y+1 and X respectively.

   [✓ c)] Y and X respectively.

   d) a port number other than Y and a port number other than X respectively.

4. In TCP timeout retransmission, the Exponential Backoff Algorithm

   a) is used to calculate RTT (Round Trip Time).

   [✓ b)] is used to calculate RTO (Retransmission TimeOut) if RTT is not available.

   c) should not be enabled due to a retransmission (Karn's Algorithm).

   d) is the random waiting time before attempting a retransmission after a CSMA/CD collision.

5. In a TCP connection, an ACK message of ack 1000 means that ____________________.

   [✓ a)] byte 999 has been successfully received

   b) byte 1000 has been successfully received

   [✓ c)] byte 1000 has not been successfully received

   d) byte 1001 is expected in the next TCP segment

6. When a sender of a TCP connection imposes Congestion Control, which parameters below are contributed by the corresponding receiver of this TCP connection?

[✓ a)] Maximum Segment Size

[✓ b)] Advertised Window Size

c) Congestion Window Size (*cwnd*)

d) Slow Start Threshold (*ssthresh*)

7. After a first TCP half close, the data transfer from the Passive Close side

a) is not allowed since this side has responded with a FIN message.

[✓ b)] is allowed with normal data acknowledgement from the Active Close side.

c) does not require acknowledgement since the other side has no data for sending ACK piggyback.

d) does not require data acknowledgement since the Active Close side has closed its half of the connection.

8. The least significant 23 bits in a 48-bit Ethernet address unambiguously identify ________.

a) an IP multicast router

b) a host

c) an IP multicast group

[✓ d)] none of the above

9. A gateway that has a pool of 4 public IP addresses needs to support 10 hosts. In order to be able to let the 10 hosts simultaneously access the network outside, the gateway must implement

a) either NAT or PAT.

[✓ b)] both NAT and PAT.

c) NAT only.

d) neither NAT nor PAT.

10. In public-key encryption, the public key can be used to ________ a message.

[✓ a)] encrypt

b) create a hash value of

[✓ c)] decrypt

d) have a digital signature encrypt in

II. A destination host receives five IP datagrams with the fields in their IP headers as shown in the table below. Identify whether each datagram is a fragment, and the sequential order for a fragment.

More Fragment	Don't Fragment	Fragment Offset	Fragment (Yes/No)?	Fragment Sequential Order (First, Middle, Last, N/A)?
0	0	512	**Yes**	**Last**
0	0	0	**No**	**N/A**
1	0	0	**Yes**	**First**
1	0	1024	**Yes**	**Middle**
0	1	0	**No**	**N/A**

III. Peter uses **tcpdump** to capture TCP segments exchanged between his machine and a remote server to open a web page by **HTTP/1.0**. He has noticed that the page is loaded with five files: a web html file and four embedded pictures. After loading the page, Peter terminates the tcpdump and examines the output. How many packets from Peter's machine should be observed with the TCP flag SYN set? How many HTTP requests from Peter's machine contain a "GET" method? Why?

Without TCP persistent connection, there are Five TCP connections established. Also, Peter's machine sent Five HTTP requests for getting five files.

IV. Both **FTP** and **TELNET** are connection-oriented applications using TCP. To grant user access, both FTP and TELNET require user ID and password to launch the respective program.

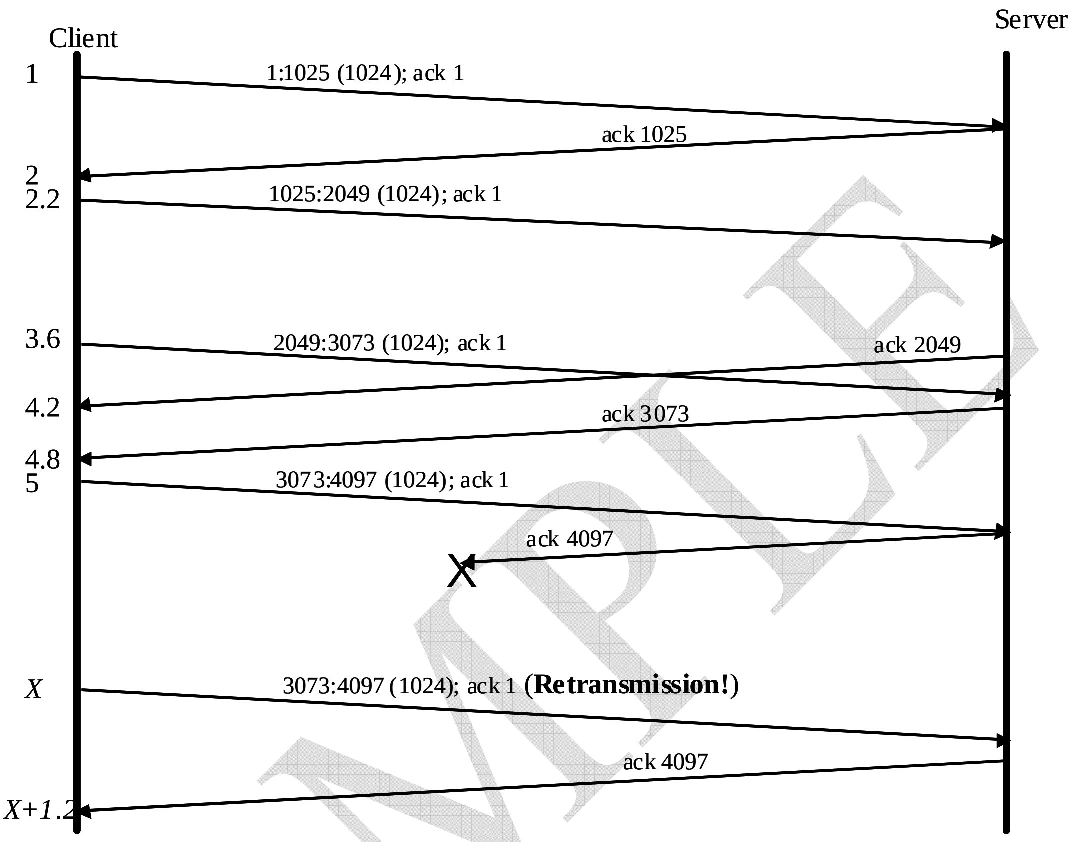
1. What is the difference between FTP and TELNET in the transmission of user ID and password?

   FTP sends login ID and password in one packet each time, while Telnet sends them by each key strike so that the information are divided into several packets.

2. In respect of the data transmission for user ID and password, which protocol is relatively more secure than the other?

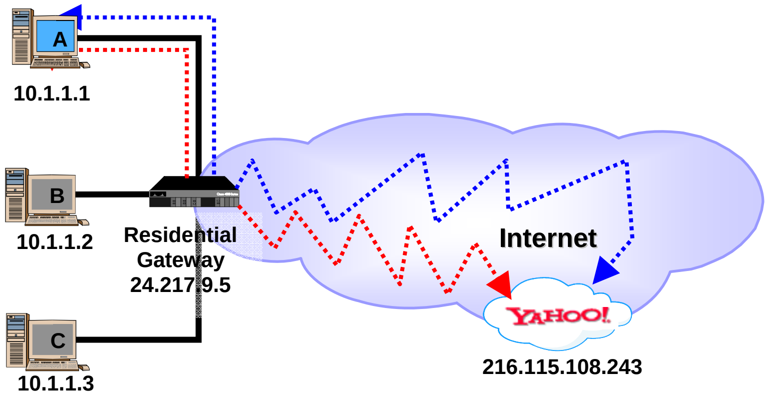
   Neither FTP nor Telnet is secure because both of them send user ID and password in plain text (no encryption used). But Telnet is more secure than FTP since it sends each key strike one by one, instead of in one packet.

V. For a TCP connection shown below, using $\alpha=1/8$, $\beta=1/4$, and G=0.1 to complete the table blow to derive the RTO values at the listed time moments based on various network conditions. Note there is NO TCP tick clock information available on the client machine. Thus your answers should be derived as floating point numbers without considering clock ticks.



Time	M (i.e. RTT)	RTT^s	RTT^d	RTO
1	-	-	-	-
2	M_0 = 1	1	0.5	3
2.2	No change in RTO since M is to be timed.			
3.6	No change in RTO since M is still running.			
4.2	2	1.125	0.625	3.625
4.8	RTO doesn't change since M is not timed.			
5	No change in RTO since M is to be timed.			
X = 8.625	The Exponential Backoff Algorithm is applied. RTO = 2*3.625 = 7.25			
X+1.2 = 9.825	No change in RTO since M is not measurable for the retransmitted segment based Karn's Algorithm.			

VI. As shown in the figure below, host A in a home LAN attempts to reach a Yahoo website at 216.115.108.243 in TWO separate sessions through a Residential Gateway (RG, a device with combined the functions of home router and DSL modem).



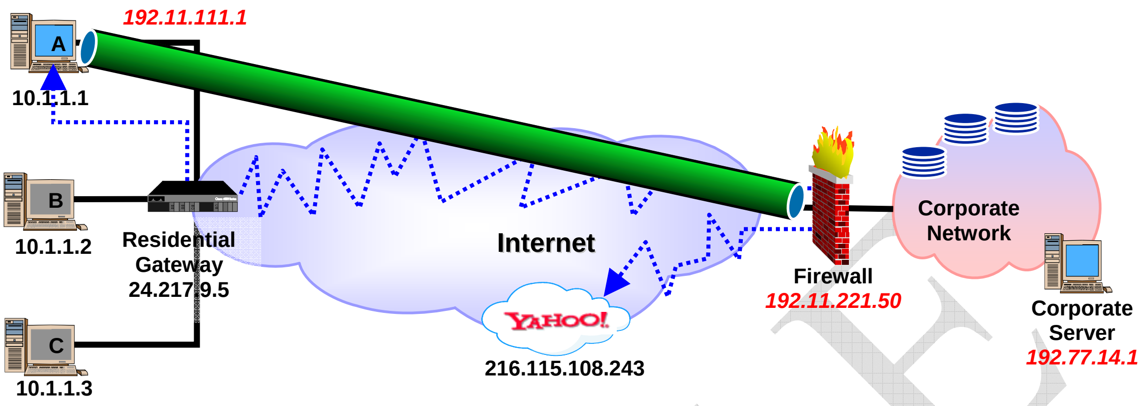
1. Suggest your own NAT/PAT bindings in the RG that make these two HTTP sessions work properly.

Binding	Private IP Address / Port Number	Public IP Address / Port Number
Session 1	10.1.1.1 / 2000	24.217.9.5/3000
Session 2	10.1.1.1 / 5000	24.217.9.5/6000

2. Based on the suggested bindings above, provide more details on IP address and TCP port number by complete the table below when host A initiates the web sessions in HTTP.

Web Session	Packet in Network Segment	Source IP Address / Port Number	Destination IP Address / Port Number
1	HTTP Request in the LAN	10.1.1.1/2000	216.115.108.243/80
	HTTP Request in Internet	24.217.9.5/3000	216.115.108.243/80
	HTTP Response in Internet	216.115.108.243/80	24.217.9.5/3000
	HTTP Response in the LAN	216.115.108.243/80	10.1.1.1/2000
2	HTTP Request in the LAN	10.1.1.1/5000	216.115.108.243/80
	HTTP Request in Internet	24.217.9.5/6000	216.115.108.243/80
	HTTP Response in Internet	216.115.108.243/80	24.217.9.5/6000
	HTTP Response in the LAN	216.115.108.243/80	10.1.1.1/5000

VII. If host A attempts to reach the Yahoo site in a web session through an existing IPSec tunnel as shown in the figure below, complete the next table with IP addresses for the IP datagrams carrying HTTP messages in the home LAN and Internet.



Web Session	Packet in Network Segment	Packet Encapsulated in Tunnel? (Y/N)	IP Header Fields	
			Source Address	Destination Address
1	HTTP Request in the LAN	Y	10.1.1.1	192.11.221.50
	HTTP Request in Internet from RG to the Corporate Firewall	Y	24.217.9.5	192.11.221.50
	HTTP Request in Internet from the Firewall to Yahoo	N	192.11.111.1	216.115.108.243
	HTTP Response in Intranet from Yahoo to the Firewall	N	216.115.108.243	192.11.111.1
	HTTP Response in Internet from the Firewall to the RG	Y	192.11.221.50	24.217.9.5
	HTTP Response in the LAN	Y	216.115.108.243/80	10.1.1.1/2000

Note: assume no NATing provided by the Firewall.