

Final Exam

CS-460

Dr Mark Clement

Name _____ SS# _____

This is a closed book, one page of notes exam. You may use a calculator if you need one. If you feel that a question is ambiguous, state your assumptions and answer the question using those assumptions.

- 1) (5 Points) How does UDP connection setup differ from the process used to set up a TCP connection? Why do these differences exist?

UDP is connectionless so you drop the listen/accept/connect part of the protocol

- 2) (5 Points) The following table has properties. For each property, indicate whether that property belongs to IPv4, IPv6, or if it does not apply to either.

Property	IPv4	IPv6
256 bit Host addresses		
Currently supported on all Internet trunks	X	
Includes site local use addresses	X	X
32 bit Host addresses	X	
The Ethernet address can be encoded as part of the IP address		X

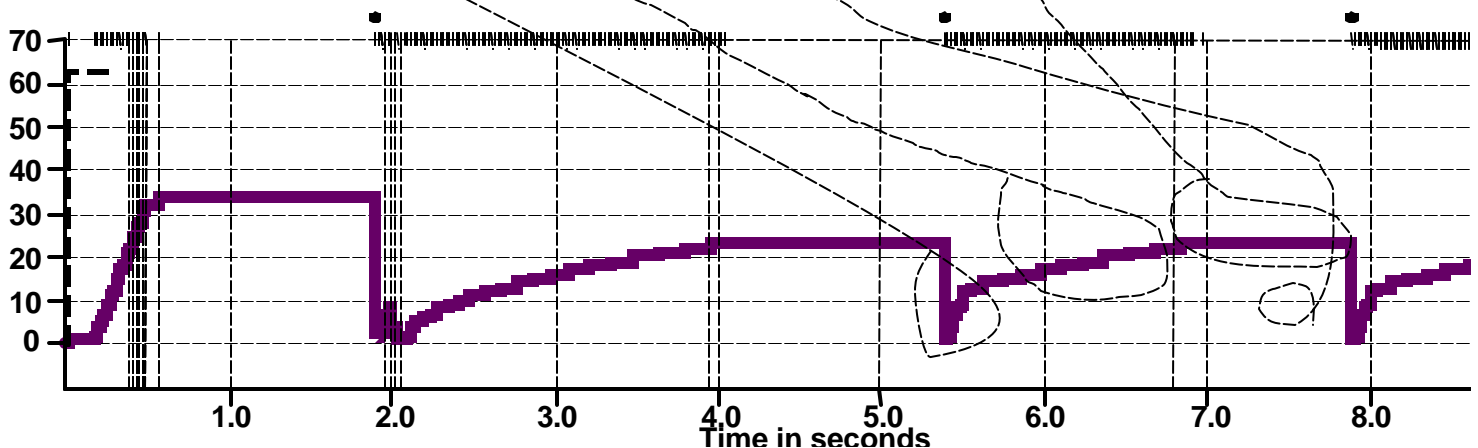
- 3) (5 Points) You are using ASN/BER encoding with an 8-bit tag field and a 1-byte length field to pass 16 bit integers in a remote procedure call (one integer per call). Assume that you are using a 9600bps modem to send the data and that there is negligible overhead in traversing the protocol stack (all of the time is accounted for by the bandwidth limitations of the network). How much time will it take to make 100,000 calls to this function?

2 bytes for encoding, 2 bytes for data, 400,000 bytes/9600bps=333 seconds

How much time would it take to make the same 100,000 calls using XDR?

No tags so 200,000 bytes/9600bps=166 seconds

- 4) (5 Points) Circle and label the Slow Start, Linear Increase, Congestion Window and Timeout Period in the following graph



- 5) (10 Points) Assume that you are using the version of TCP with sizes much larger than 64kb that implements Slow Start. Suppose that you are using this extended TCP over a 155Mbps link with a RTT of 300ms to transfer a 100MB file, and the TCP receive window is 20MB. If TCP sends 1500B packets, and assuming no congestion and no lost packets:

How many RTTs does it take until the sender's congestion window reaches 20MB? (Recall that the congestion window is initialized to the size of a single packet)

Starting from a window of 1 packet, 1500B, 3000B, 6000B, 12KB, 24KB, 48KB, 96KB, 192KB, 384KB, 768KB, 1.5MB, 3MB, 6MB, 12MB, 24MB = 14RTT (20MB/1500B=13.9Kpackets, log base 2 of 16K=14)

The delay-bandwidth product is actually less than 20MB, so if they notice this and cap it lower, that answer is acceptable too.

How many RTTs does it take to send the file?

In this time, we have sent about 24MB of data (before the 24MB segment was sent)
100MB-24MB=76MB left to send at 20MB per RTT=4RTT

Total time 18RTT

If the time to send the file is given by the number of required RTTs times the link latency, what is the effective throughput for the transfer?

Total time 18RTT=18*300ms=5.4sec

What percentage of the link bandwidth is utilized?

Effective Throughput=100MB/5.4sec =18.5MBps =148Mbps

- 6) (5 Points) Assume that there is a maximum latency of 20ms for each router in the internet. What is the maximum time between when a IPv4 packet is sent and when it is received given that the maximum latency between routers is 210ms (since the packet could go through a satellite on every link).

Max TTL=255*230ms=58seconds or about the minute that we assume packets can be alive on the internet

- 7) (5 Points) What is DNS and what are the steps used to resolve the name xr5.xenon.aol.com from the machine trunk.cs.byu.edu.?

Domain Name System, contact root server to get name of byu.edu, contact byu.edu name server to get cs.byu.edu, contact cs.byu.edu name server to get trunk.cs.byu.edu

How is load balancing performed between several web servers using DNS?

The name server returns multiple IP addresses (round robin reordering) for one name and the browser can pick one of them

8) (5 Points) Identify the properties of canonical-intermediate-form and receiver-makes-right .

Property	canonical -intermediate -form	receiver-makes-right
Routing protocol for switches		
Used by IP	X	
A Pentium would have to convert all integers	X	
Requires N*N transformations if there are N machine types		X
Used to make sure big endians and little endians get along	X	X
All data on the wire has the same endian-ness	X	

9) (5 Points) Describe the following TCP flow control algorithms

a. Slow Start

Start at one, exponential increase until congestion window, linear increase until packet drop, set congestion window to half of value when packet was dropped

b. Fast Retransmit

Don't wait for timeout, retransmit when receive multiple acks for same sequence number

c. RED

Random Early Detection – drop with increasing probability as queue size increases but before overflow

10) (5 Points) Indicate which properties belong to DES and RSA encryption.

Property	DES	RSA
Faster and can achieve higher bandwidth	X	
Has a private key and a public key		X
Can be used to perform a secret key exchange		X
Computes the cryptographic checksum for a block of data		
Performs permutations and xor operations in order to encrypt	X	

11) (5 Points) You are using MD5 with RSA in order to send a message. The sender transmits $\langle \text{message} + E(E(\text{MD5}(\text{message}), \text{publickey}_{\text{receiver}}), \text{privatekey}_{\text{sender}}) \rangle$. Suppose that some intermediate party wants to modify the message without the receiver detecting it. What would this intermediate party have to do? How hard would this be?

Would be able to decrypt $E(\text{MD5}(\text{message}), \text{publickey}_{\text{receiver}})$ using the public key of the sender, but would not be able to decrypt the $E(\text{MD5}(\text{message}))$ unless the private key of the receiver were cracked. This should be really hard. Even if this were completed, the private key of the sender would be needed to change the MD5 checksum

12) (5 Points) Describe the 7 steps in exchanging a PEM message.

- Random k, encrypt with DES, Encrypt k with receivers public, encode message in ascii,
- Convert from ascii, decrypt k with receivers private, decrypt with DES

13) (10 Points) Given $p=101$, $q=113$, $e=3$ find the decryption exponent d for RSA. (Hint: Although there are methodical ways to do this, trial and error is efficient for $e=3$)

$d = \underline{\hspace{2cm}}$

$3d \equiv 1 \pmod{(p-1)(q-1)} = 1 \pmod{100 \cdot 112} = 1 + 11200k$ for some k . $k=2$ works and $d=7467$

Compute the RSA cyphertext for a message value of 9876 (Note that evaluating m^3 with 32 bit arithmetic results in overflow.

$c = \underline{4906}$ $m^3 = m^2 m = 11291 \cdot 9876 = 4906 \pmod{11413}$

14) (10 Points) Assume that the following tables contains the DCT for a macroblock of a JPEG file and the quantization table. Create a reasonable Huffman coding for the values you need and then show the RLE of the resulting macroblock.

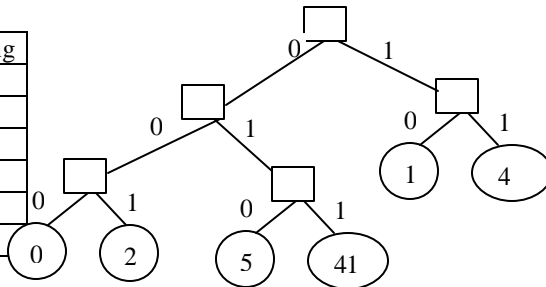
DCT			Quantization		
124	56	13	3	15	29
78	32	6	15	29	65
21	4	2	29	65	85

41	4	0
5	1	0
1	0	0

RLE=1-41,1-4,1-5,2-1,4-0,

Huffman encoding

Symbol	Weight	encoding
1	4	10
4	2	11
41	1	011
5	1	010
2	1	001
0	1	000



RLE=10 011 10 11 10 010 110 10 11 000=1001 1101 1100 1011 0101 1000=0x9dcb58

15) (5 Points) Give the Lempel-Ziv compression for the string "abbbabbaababbabaaabaabba"
 compression encoding = 0,1,3,2,1,0,2,5,8,7,6,9
 a b bb ab b a ab abb aba aa ba abba

index	entry	index	entry	index	entry
0	a	5	abb	10	abaa
1	b	6	ba	11	aab
2	ab	7	aa	12	baa
3	bb	8	aba	13	
4	bba	9	abba	14	

16) (10 Points) Show the steps in building the link-state routing table for Node D.

Step	Confirmed	Tentative
1	(D,0,-)	
2	(D,0,-)	(A,2,A)(B,2,B)(E,5,E)
3	(D,0,-)(A,2,A)	(B,2,B)(E,5,E)
4	(D,0,-) (A,2,A) (B,2,B)	(E,4,B)(C,6,B)
5	(D,0,-) (A,2,A) (B,2,B) (E,4,B)	(C,5,B)
6	(D,0,-) (A,2,A) (B,2,B) (E,4,B) (C,5,B)	
7		
8		
9		
10		

