

Final Exam

*Open book and notes; In class**Friday, Dec 20th*

- ⊕ *Do not forget to write your name on the first page. Initial each subsequent page.*
- ⊕ *Be **neat** and **precise**. I will not grade answers I cannot read.*
- ⊕ *You should draw simple figures if you think it will make your answers clearer.*
- ⊕ *Good luck and remember, brevity is the soul of wit*

- All problems are mandatory
- I cannot stress this point enough: **Be precise**. If you have written something incorrect along with the correct answer, you should **not** expect to get all the points. I will grade based upon what you **wrote**, not what you **meant**.
- Maximum possible points: 50.

Name: _____

Problem	Points
1	
2	
3	
4	
5	
Total	

1. Nomenclature

(a) Describe the following: (2 points each)

- Zone Transfer
- Extended Service Set (802.11)
- CSMA-CD
- CNAME Resource Record
- Hidden Node Problem

2. Network and Transport

(a) Construct an example where the MED attribute is used for BGP best path selection. (3 points)

(b) In TCP Fast Recovery, after the retransmission upon the third duplicate ACK, $\text{cwnd} \leftarrow \text{ssthresh} + 3 \cdot \text{MSS}$. What is (a) the value of **ssthresh** at this point, and (b) why the extra 3 MSS? (3 points)

a)

b)

(c) Construct an example (with two space-time diagrams) where Selective Acks are more efficient than Cumulative Acks. You may use variables to represent sequence numbers if helpful. Smaller (correct) examples get more points. (4 points)

MAC Protocols

- [illegible]

4. Application Layer

- (a) In steady state, how does a unmodified BitTorrent peer choose which six nodes to upload data to? (3 points)
- (b) In modern protocols, why is conveying network layer information(such as the network address) within the application payload considered to be poor design? (3 points)
- (c) Suppose you are a user-car salesman accepting BitCoins to increase business. How long do you have to wait before it is safe for you to release a car after receiving coins? Why? (4 points)

5. General

- (a) What divisor polynomial degenerates CRC codes to parity codes? How? (3 points)
- (b) The *Hamming Distance* between two bit strings A and B is the number of bits that have to be changed in A to obtain B. The CRC-32 polynomial $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ is used in Ethernet. Prove the following statement or disprove it with a counter example: “The minimum Hamming distance between two valid messages using the CRC-32 ethernet polynomial is 16”. (3 points)
- (c) BitCoins require continuous energy expenditure from an honest majority for the block chain to remain valid. Describe an alternative that does not. You will be graded on the inventiveness of your design along with how well you analyze both its pros and the cons. (4 points + Bonus)

Bonus What was Galois’ first name? (1 point)