CMSC 417 Computer Networks **Spring 2013**

Final Exam

Open book and notes; In class *Saturday, May 11th*

⊕ *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)

   - Cyclic Redundancy Check

   - Onion Routing

   - CSMA-CA

   - Diffie-Hellman Protocol

   - Exposed Node Problem

2. Network and Transport

(a) What problem does CIDR solve? (2 points)

(b) What is the `TCP-NODELAY` option useful for? What does it do? (2 points)

(c) Why did the D-root server change IP addresses from 128.8.10.90 to 199.7.91.13 to support anycast? (3 points)

(d) Would it have been *possible* to anycast the D-root server without renumbering? If yes, how? If not, why not? (3 points)

MAC Protocols

3. (a) The minimum frame size in 802.3 (Ethernet) was 64 bytes. This limited the maximum (physical) network length to 2500 meters. Why? (3 points)

(b) What protocol feature would you enable/disable to set up a "hidden" 802.11 network? (2 points)

(c) Why does 802.11 include an ACK but 802.3 does not? (2 points)

(d) Why does a 802.11 node that joins the network have to wait DIFS time before transmitting even if the medium is free? Describe in terms of the states other nodes may be in. (3 points)

4. Application Layer

   (a) How are MX records used in sending electronic mail? (2 points)

   (b) What is the INV message in Bitcoin used for? What message is used to respond to an INV? (2 points)

   (c) The stabilize protocol in Chord at node n is:
   `x` $\leftarrow$ `succ.pred; succ` $\leftarrow$ `x if (x` $\in$ `(n, succ)); succ.notify(n);`
   The notify function at node n with n' as input is defined as:
   `if (pred is` $\perp$ `or n'`$\in$`(pred, n)) pred` $\leftarrow$ `n'`
   Can the `stabilize` protocol in Chord "heal" the ring if a node departs? How/Why not? (2 points)

   (d) Suppose a Chord ring is stable, with n_0, n_1, n_2, n_3 in a row (i.e., n_{i-1} is n_i's predecessor, and n_{i+1} is n_i's successor. Suppose each node maintains information about one predecessor, and three successors. Node n_2 dies. Show a sequence of calls and show the state of the pred./successors that correctly reconstructs all succ./pred. pointers.

5. General

(a) 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". (2 points)

(b) Describe how the TOR circuit creation protocol can be compromised if standard Diffie-Hellman (without signatures) is used to exchange keys. How does TOR solve this problem? (3 points)

(c) Suppose you have a stable DHT with 10^6 nodes. Node x wants to send a stream of messages to a set R with 10^4 other nodes. A message arrives at x every millisecond, and each message requires one millisecond to transmit (a node may transmit simultaneously to four other nodes at any one time).

Use the DHT to design a protocol by which x can send m messages to the set R such that the maximum delay for any message from x to any node in R is independent of m. You will be graded on the efficiency of your protocol, and your analysis of its correctness/guarantees. (5 points + Bonus)