

EECS 3214 Final Exam
Winter 2017
April 19, 2017
Instructor: S. Datta

Name (LAST, FIRST): _____

Student number: _____

Instructions:

1. If you have not done so, put away all books, papers, and electronic communication devices. You may keep your calculator. Write your name and student number now.
2. Check that this examination has 12 pages. There should be 20 questions worth 80 points.
3. You have 180 minutes to complete the exam. Use your time judiciously.
4. Show all your work. Partial credit may be given for an answer, but only if you show the intermediate steps in obtaining the answer.
5. If you need to make an assumption to answer a question, please state the assumption clearly.
6. Your answers MUST be LEGIBLE.

Answer the questions in the spaces provided on the question sheets. If you run out of room for an answer, continue on the back of the page.

5. (4 points) Suppose that your company sells online pay-per-view subscriptions to concerts. Based on your study of network security, list some issues involved in designing a secure, effective system for this purpose and sketch the security features you would use in such a system.
6. (4 points) What information does each node transmit in every round of the Distance Vector algorithm? Give two primary advantages and one serious disadvantage of using Distance Vector algorithms in intra-AS routing.

7. (4 points) List the two records that are required at a minimum to add a web server (say for a new company) to the Internet.

8. (4 points) Consider a part of a routing table that looks as follows:

Prefix match	Link interface
255.128.0.2/24	0
255.128.0.128/25	1
255.128.0.64/25	2
otherwise	3

What link interface is a packet with destination address 255.128.0.2 sent to? You must give reasons to get credit for your answer. In case you forgot, here are the powers of 2: $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, $2^8 = 256$.

9. (4 points) Based on your study of the upper layers of the TCP/IP architecture, what are the difficulties in identifying the source of a packet sent over the Internet? If you were allowed to make small modifications to the architecture, what changes would you propose to aid in locating the source of a set of malicious packets on the Internet?
10. (4 points) What are BGP sessions and how are they implemented? Does this violate the order of the 5 layers in the TCP/IP architecture? Why?

11. (4 points) Consider two TCP sessions, S_1, S_2 such that S_1 goes through bottlenecks b_1, b_2 but S_2 only goes through bottleneck b_1 . Argue that S_1, S_2 do not eventually get equal shares of bandwidth in bottleneck b_1 . Generalize the reasoning to argue that TCP is unfair to long paths.
12. (4 points) What is the fast retransmit algorithm in TCP? What are the motivations for using it?

13. (4 points) Describe how a weighted fair queuing scheduler works. How does it result in guaranteed bandwidth for a class of traffic?

14. (4 points) Describe how forward error correction and interleaving are used together to alleviate the effect of packet losses in multimedia networking

15. (4 points) What changes at the core and edge does the DiffServ architecture propose to make?

16. (4 points) How does jitter impact multimedia communication? Outline the algorithm described in class for adaptively setting playout delay of multimedia streams.

17. (4 points) Describe how SIP enables locating the IP address of a user from their email address, so that VoIP calls can be placed to an email address.

18. (4 points) Why does the session initiation protocol (SIP) allow the sender and receiver to choose two different multimedia encoding schemes? Describe one scenario where it makes sense to use different encoding protocols at the sender and receiver.

19. (4 points) Why is RSA believed to be hard to break, i.e., the complexity of what computational problem leads to the belief that it is secure? RSA can be used to authenticate messages by concatenating to the message its ciphertext encrypted with RSA using the private key of the sender. Why is this not commonly done in practice?
20. (4 points) What are the security risks of DNS, i.e., what damage could an adversary do by exploiting DNS? How can these threats be addressed by incorporating security into DNS?

Use this page if you need extra space. Mark the question number clearly.
--