College of Computing

Georgia Institute of Technology

CS 3251: Computer Networking: Spring 2013

Quiz II

There are 12 questions and 12 pages in this quiz booklet (including this page), plus one optional bonus question. **There are 90 total points.** Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

The last page is an easy, optional set of questions. *Rip this page off of your exam for five bonus points.* Turn it in anonymously.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If I can't understand your answer, I can't give you credit!

Use the empty sides of this booklet if you need scratch space. You may also use them for answers, although you shouldn't need to. *If you do use the blank sides for answers, make sure to clearly say so!*

Note well: Write your name in the space below AND your initials at the bottom of each page of this booklet.

THIS IS AN "CLOSED BOOK" QUIZ.
NO BOOKS, NO NOTES, NO OTHER MATERIALS, NO PHONES, NO COMPUTERS, NO LAPTOPS, NO PDAS.
ONE TWO-SIDED LETTER-SIZED NOTE SHEET IS ALLOWED. MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!

Initial here to indicate that (1) you've read the instructions and (2) you agree to abide by the Georgia Tech Honor Code:

Do not write in the boxes below

1-5 (xx/20)	6-8 (xx/18)	9-10 (xx/21)	11-13 (xx/23)	14 (xx/8)	Bonus (xx+5/10)	Total (xx/90)

Name:

I Warmup

1. [4 points]: Which of the following is true about content distribution networks?
(Circle ALL that apply)

A. Content distribution networks can improve the performance that a client sees by reducing the network latency between the client and the content that it is downloading.

B. Content distribution networks can reduce transit expenses for a content provider by enabling much of the provider's content to be served from a nearby network, sometimes even from a cache that is within the client's own network.

C. Content distribution networks typically redirect Web clients to a nearby Web cache by rewriting the IP address of packets sent from the client to the IP address of the nearby Web cache.

D. Real-time content such as video streams cannot be distributed from a content distribution network.

E. All of the above.

2. [4 points]: Which of the following are true about 802.11 wireless medium access control?
(Circle ALL that apply)

A. A wireless sender can avoid causing a collision at the receiver by performing a "carrier sense" to determine whether any other sender wants to transmit at the time that it wishes to send a packet.

B. Using RTS/CTS ("request to send", "clear to send") control reduces the overall achieveable throughput of the wireless network.

C. Only wireless networks can have collisions at the receiver; such collisions are not possible on wired Ethernet networks.

D. Disabling RTS/CTS necessarily lowers the effective throughput of the wireless network, since more collisions will occur at the receiver without RTS/CTS enabled.

E. All of the above.

3. [4 points]: Which of the following are true about video streaming?

(Circle ALL that apply)

A. Using TCP for video streaming could result in larger delays between transmission and playout than streaming the same video with UDP.

B. Since UDP provides no reliable delivery guarantees, a video streaming application that uses UDP as its transport cannot recover from any packet loss in the video stream.

C. A larger playout buffer at the client allows the client more time to recover from lost packets.

D. Using UDP to stream a video instead of TCP is appropriate if the client is more concerned about low delay and interactivity than it does about receiving a high-quality stream.

E. All of the above.

4. [4 points]: Which of the following are true about TCP?

(Circle ALL that apply)

A. TCP guarantees that the receiver sees the same in-order stream of bytes that the sender transmitted.

B. A TCP sender controls its sending rate by adjusting the number of unacknowledged packets that can be sent over the network at any time.

C. TCP's congestion avoidance algorithm causes the sender to reduce its sending rate by a factor of two when it sees a packet loss.

D. A TCP sender and receiver use a "three-way handshake" both to set up and to terminate the TCP connection.

E. All of the above.

5. [4 points]: Which of the following are true about the denial of service attacks (and defenses) that we discussed in class?

(Circle ALL that apply)

A. In a "SYN Flood" attack, each TCP SYN packet that a victim receives causes the to set up TCP connection state.

B. A "DNS Reflection" attack requires the attacking client to "spoof" the source IP address of the packet containing the DNS request.

C. If every network on the Internet performed stateless *ingress* filtering to defend against source IP spoofing, the DNS reflection attack that we discussed in class would not work.

D. If every network on the Internet performed stateless *egress* filtering to defend against source IP address spoofing, the DNS reflection attack that we discussed in class could not be carried out.

E. All of the above.

Initials:

II DHCP and NAT

6. [4 points]: Suppose a network has a /24 IP prefix (256 IP addresses). The network has 1,000 devices, but no more than 200 of them are active at any time. Explain how a network operator can use DHCP to give a unique IP address to each client.

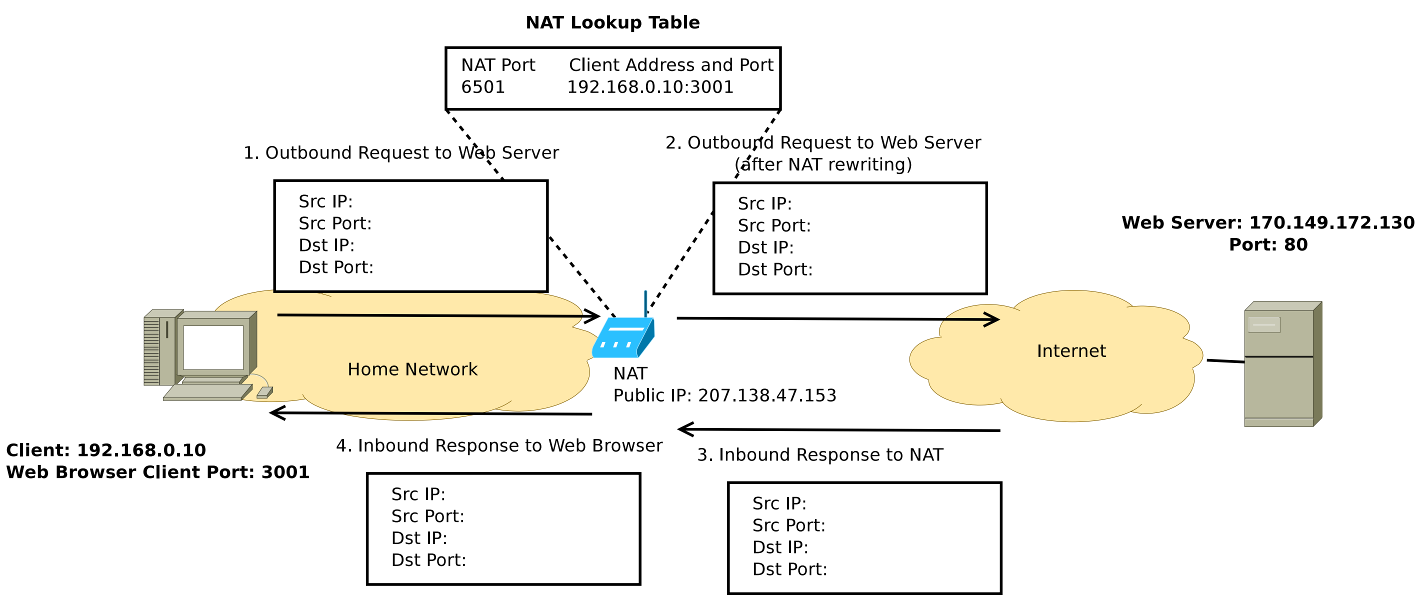
(Answer legibly in the space below.)

7. [4 points]: Suppose instead that in the /24 network above, *500 devices* are active at any given time. Explain how a network operator could use a single NAT (network address translator) to allow the devices on the network to connect to the network simultaneously, even though there are now more simultaneously active devices than available public IP addresses. (You may find it helpful to use a diagram to explain your answer.)

(Answer legibly in the space below.)

Initials:

8. [10 points]: Consider the figure below, which shows a home network that is connected to the Internet by a NAT device. We have shown the lookup table that the NAT maintains for a particular device in the home network, which maps each port number to a private IP address and port for some device “behind” the NAT into the home.



- Briefly explain the why NAT devices need a lookup table, and how this lookup table would be populated.
- Given the lookup table we provided, fill in the missing source and destination IP and port numbers on *all four packets* in the diagram above, when the client in the home attempts to send a packet to a Web server on the Internet.

Initials:

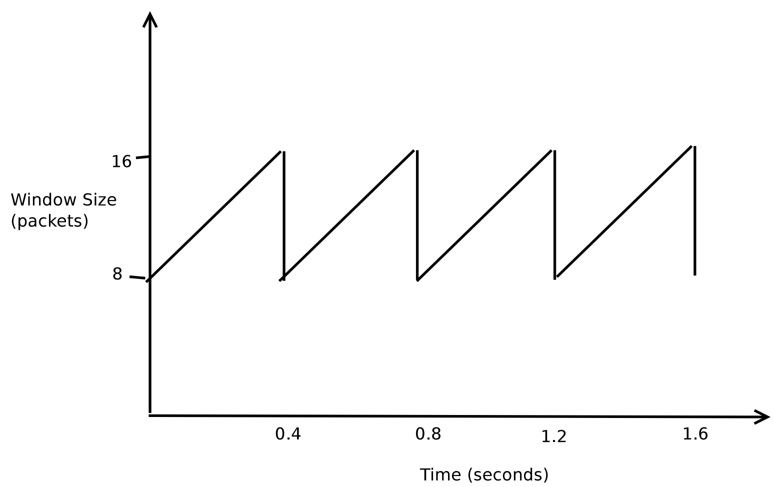
III TCP Congestion Control

9. [5 points]: Suppose that, at a given time, a TCP sender has a congestion window of 10 packets, that each packet is 1500 bytes, and that the round-trip time between the sender and receiver is 100 milliseconds. What throughput can the TCP sender achieve? *Give your answer in bytes per second and show your work.*

(Answer legibly in the space below.)

Initials:

10. [16 points]: Consider the "TCP sawtooth" below, which shows the evolution of the TCP congestion window size for a sender over time. Assuming this TCP connection is using the usual additive incraese multiplicative decrease (AIMD) congestion control algorithm. *You may need the back of a page to answer some of this question. If you need more space, please indicate where we can find your answer, such as on the back of this page.*



(a) Draw arrows on the diagram where packet loss occurs. Clearly label your arrows with the text "packet loss" so we know what you're pointing at.

(b) What is the round trip time between the sender and receiver? Briefly show your work/explain your answer.

(c) Assuming *1000-byte packets*, what is the average sending rate of the sender, in bytes per second? (You can assume that the y-axis on the diagram is to scale, and you can give your answer either numerically or graphically. If you can't compute the rates in bytes per second, give the average window size for partial credit.)

(d) Suppose that the data being sent over this connection is a video stream, and that the receiver wants to ensure "smooth" playout. What is the minimum amount of buffering that the client should have to ensure that the receiver can play out at the average rate, without interruption? A numerical answer is better (show your work), but if you cannot figure out the math, you can give an answer graphically.

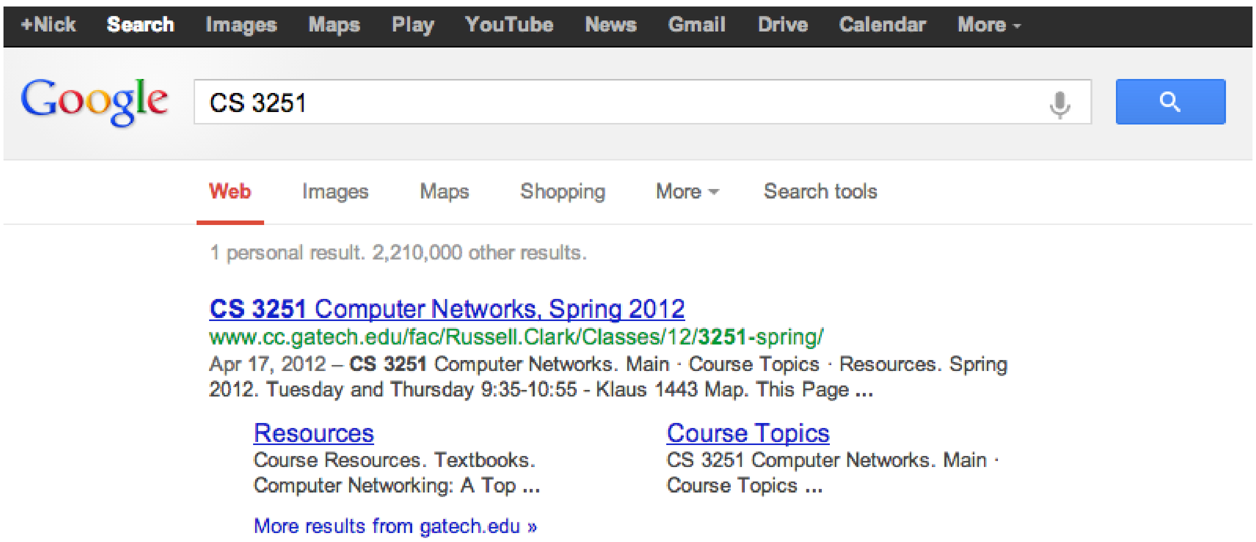
(Answer legibly in the space below.)

Initials:

IV Web Performance and Caching

11. [4 points]: Consider the Web page shown below. Circle the parts of the page that most likely can and should be cached on a local cache in a content distribution network. *Explain your answer.*

(Answer legibly in the space below.)

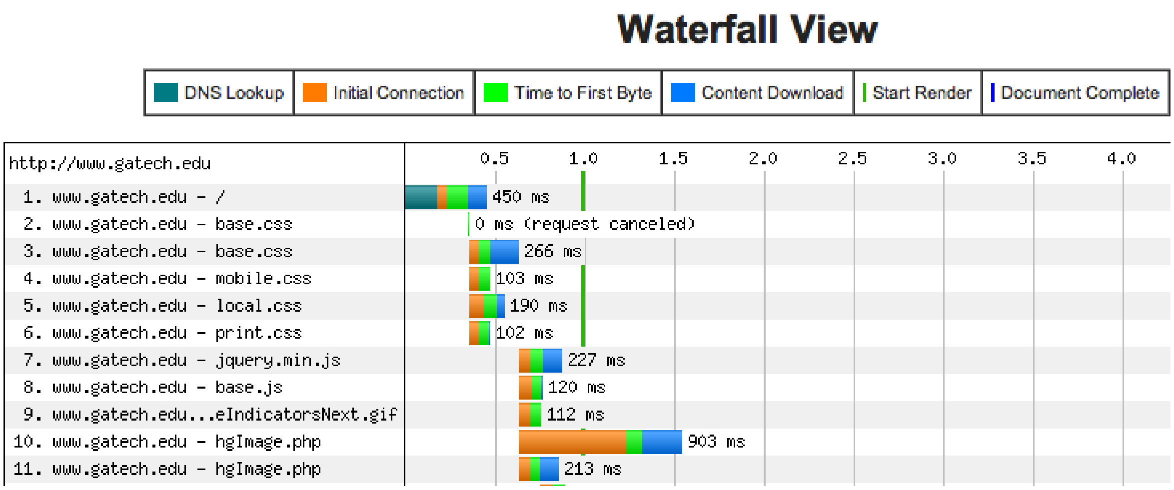


12. [4 points]: Suppose that a typical Web browser can open multiple TCP connections in parallel *to each unique domain name*. Describe how a Web site designer might use the DNS to name Web objects so that such a client browser might load the page more quickly.

(Answer legibly in the space below.)

Initials:

13. [15 points]: Consider the partial waterfall diagram below, for `http://www.gatech.edu/`.



(a) How many TCP connections does this Web browser open in parallel?

(b) Which object downloads benefit from DNS caching? (You can use the object numbers in your answer to save writing.)

(c) Explain why persistent HTTP connections can reduce overall page load time, when they are used. Does the Georgia Tech site use persistent HTTP connections? How can you tell?

(Answer legibly in the space below.)

Initials:

V Firewalls (+ Bonus Design Question)

Suppose that Georgia Tech wants to only allow access to some of its Web content for clients who are on campus. (For example, Georgia Tech might post a video stream that it wants to ensure is only visible on campus.)

To do so, it implements a stateless IP-based firewall that checks the source IP address of the Web client making the HTTP request and sends a TCP "reset" to any client whose source IP address is not inside of the Georgia Tech network.

14. [8 points]: George Burdell is graduating next month and wants to continue to be able to download this "Georgia Tech only" content, even after he gets out. He thinks that a carefully positioned Web proxy could help him evade Georgia Tech's IP address-based filter. Explain where George should deploy his proxy, with respect to the client and the Web site, and how the proxy could defeat the IP-based firewall.

(Answer legibly in the space below.)

15. [5 points]: Bonus!! Optional! The Georgia Tech Office of Information Technology notes that you've completed CS 3251 and wants to hire you to ensure that people like George can't continue to download "GT only" content, even in the presence of Web proxies. Explain how you might design a more sophisticated firewalling system to detect that client requests like George are being sent through a proxy, as opposed to originating directly from the client.

(Answer legibly in the space below.)

Initials:

Congrats! + Feedback + Thank You

This page is anonymous. Rip this off from your exam, and turn it in separately if you like. You'll get five points for simply ripping off the last page of the exam, but I'd prefer if you fill it out and hand it in in a separate stack.

Congratulations on finishing! Thank you for taking this course with us. We have really enjoyed the pleasure of teaching it, and we have enjoyed your enthusiasm for the material. We know that not everything has been "easy", but we hope that now that the course is over, you will walk away with some useful knowledge and experience that you will use in the future, and will remember us fondly. :-)

What was the best part of the course? Anything is fair game here (topics, course structure, board technique, etc.).

What was the part of the course you'd like to see improved (or removed)?

What was the best thing you learned in this course?

What part of the course was not useful, in terms of your learning (if any)?

In future offerings, what single thing would you recommend to improve the course?

Have you filled out CIOS? If "no", please do it soon. We will remind you at the project demos. :-)

Initials: