CS 447-Networks and Data Communications
Final Exam
Fall, 2015

10:00-11:40 A.M.
December 17, 2015

This exam is a closed-book and closed note exam. There are 8 questions in this exam. You have 100 minutes to finish the questions. Please write your answers on separated piece of papers. To avoid grading problems, please staple your papers in the ascending order in the question number. Calculator can be used during this exam, but you can not share a calculator with anyone else.

Your last 3 digits: _____

QUESTION #1 (4 points for each, 15 minutes)

(1) What are "blocking services (in telecommunication)" (definition of "blocking services")? Mention one example of blocking telecommunication services.

(2) What are the primary advantages (two advantages) and disadvantages in "datagram packet-switching networks"?

(3) What is "packet encapsulation"? What is it for (i.e., What is the purpose of "packet encapsulation")?

(4) What are the major advantages in using "network protocols"? What are the major disadvantages in using "network protocols"?

(5) For each of the following factors, what ("increase" or "decrease") should we (i.e., computer scientists) do to increase the expected link bandwidth utilization?

(a) Transmission rate (in bps):

(b) Packet size (in bytes per packet):

(c) End-to-end logical link distance (in miles):

(d) Signal propagation speed (in miles per second):

QUESTION #2 (4 points for each, 15 minutes)

(1) For high-error rate (but relatively low transmission rate) transmission links, which of "GBN ARQ" or "Selective-Reject ARQ" is better? Justify your choice.

(2) Visualize the structure of "error control" for packet-switching networks by completing the following tree diagram.

(3) Why does each IP address consist of two addresses of "domain address" and "host address" (what is the motivation behind the design)?

(4) Why are "MAC addresses" used (needed), while the Internet Protocol uses "IP addresses"

(5) What is "IP address" (what does each IP address represent)?

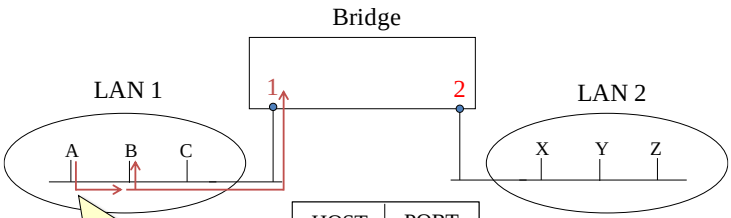
QUESTION #3 (4 points for each, 15 minutes)

(1) ARP can not discover the MAC address of any destination host computer in remote domains. If a destination of an IP packet is to a remote domain, what will ARP do?

(2) (Homework Research) Mention two interior routing protocols and one exterior routing protocol.

(3) Let us assume that the two LAN segments are connected by a switch as shown by a figure below. At the beginning, the table is empty. After the following activities, show the contents of the table (after the initial state).

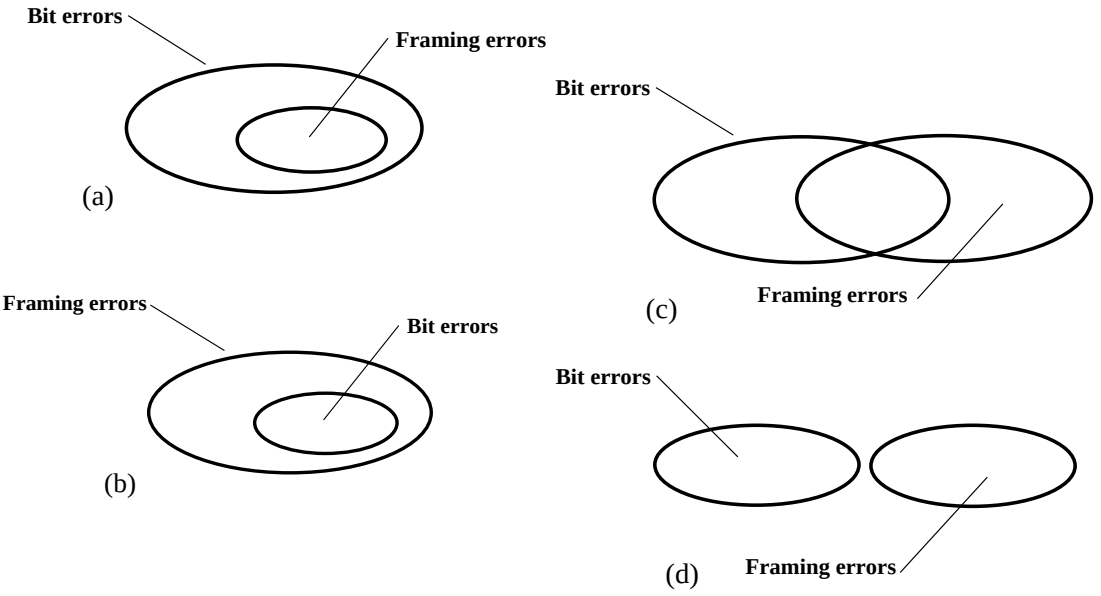
- A sends a message to B (but B has not replied to A yet after a sends the message)
- Y sends a message to Z (but Z has not replied to Y)
- Z responds to Y's message



HOST	PORT
A	
B	
C	
X	
Y	
Z	

(4) What is the primary advantage and disadvantage of "1-persistent" CSMA/CD medium access control?

(5) The followings are Ven Diagrams that try to show the relationship between bit errors and framing errors. Which one(s) is correct (select <u>all</u> that are correct)?



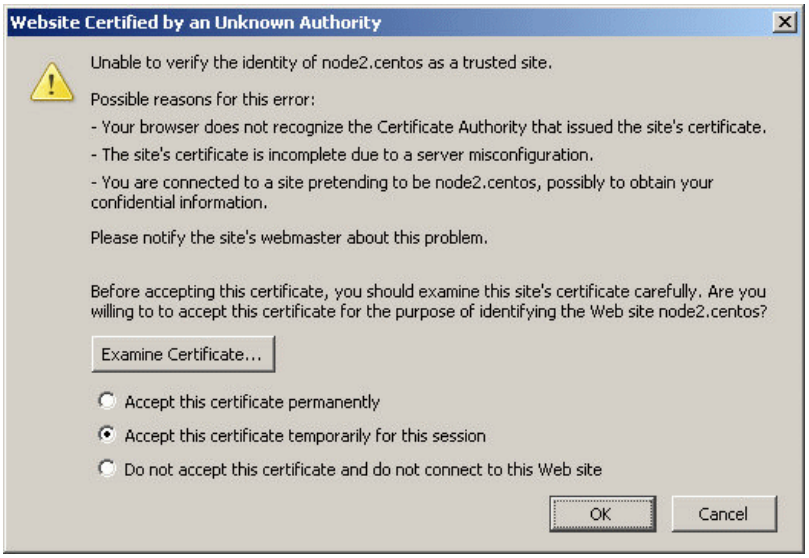
QUESTION #4 (4 points for each, 15 minutes)

(1) Why are "DDoS attacks using botnets" hard to stop? Mention two major different reasons.

(2) What does "digital certificate" certify?

(3) Describe the procedure a home user's local web browser performs (from the time a home user's local web browser receives a digital certificate until it confirms the validity of a public key).

(4) What does the following warning message is warning you against (technically describe what the local web browser has detected)?



(5) Regarding digital signature, why is it necessary to encrypt the message digest by the private key of a sender? Select the most appropriate type of threats from the options below (the best option – please do NOT select more than one).

(a) man-in-the-middle attacks
(b) replay attacks
(c) release of message contents attacks
(d) masquerade attacks
(e) traffic analysis attacks
(f) denial of service (DoS) attacks

QUESTION #5 (4 points for each, 10 minutes)

(1) Why is "end-to-end delay" usually unpredictable in the Internet (technically explain)?

(2) Which of the following QoS metric is essential for VoIP (Voice over IP) network applications? Select the most essential metric (select one).

(a) Transmission rate

(b) Packet-loss late

(c) End-to-end delay

(d) Delay jitter

(3) Motion pictures (video) using MPEG (MP3 and MP4) encoding are considered inelastic VBR traffic. Technically describe how they have "VBR" traffic.

(4) Which QoS metric(s) traffic policing will effectively control (select all that apply from the followings)?

(e) Transmission rate

(f) Packet-loss late

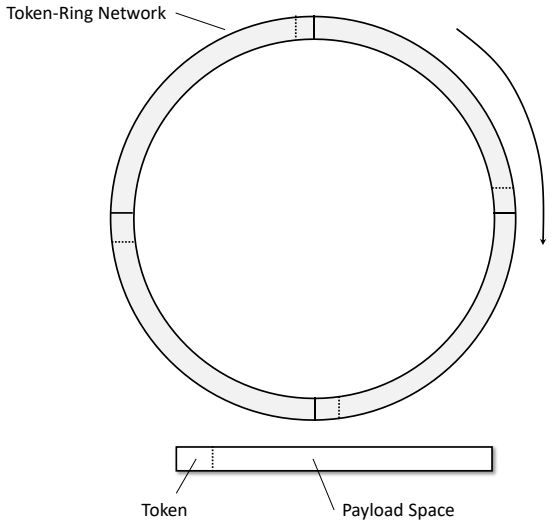
(g) End-to-end delay

(h) Delay jitter

(5) What is "signaling"?

QUESTION #6 (20 points, 10 minutes)

The throughput of token-rings can be improved in the following way. Instead of circulating only one token in a ring, multiple tokens can be circulated in a ring network at a time. Following each token is the empty space, called payload space. Each token has the empty flag inside of each token. A transmitting host waits for a token that has the empty flag = 1 (TRUE). Then, a transmitting host changes the flag from 1 to 0 (FALSE – means occupied) and then insert payload right after the token. Each token has ACK field (as we discussed). The host waits for the token to which it inserted its payload to come back. The host finally sets the empty flag = 1 when the token (followed by its payload) to come back. Multiple tokens exist with the same interval in a ring.



With the following assumptions, find the throughput (in bps) of this improved multiple-token-ring networks. Show all your work (in a quantified way).

- Transmission rate = 1Gbps (1G = 10^9)
- Signal propagation speed is 200m/μs
- Each repeater inserts 100-bit delay
- There are 50 repeaters in a ring.
- The link distance between two repeaters is 30,000m.
- There are 100 tokens in a ring, and each token is 100 bytes (800 bits).

QUESTION #7 (20 points, 10 minutes)

Show how CRC error check works by demonstrating its working (both at the sender and the receiver sides) for the following case:

Payload bits: "111110110"

Detection key: "1011"

QUESTION #8 (20 points, 10 minutes)

Let us assume that two corporate organizations have business transactions between them. One of the two, called 'A', is a manufacturing company, who buys parts from the other, called 'B', who is a part supplier to 'A'.

'A' regularly orders a particular product 'X' to 'B'. 'A' sometimes makes orders for 'X' to 'B' a couple of times even on the same day.

Question: Design a secure network application that guarantees "sender-side non-repudiation (sender can not deny what he has sent)" for 'B'.

Requirement: Each order from 'A' to 'B' should be performed as one message.

Assumptions:

- You can assume that whatever necessary encryption keys (symmetric key(s) and/or public key(s)) and digital certificates have been exchanged between 'A' and 'B' in advance – but please clearly state which have been, in your design.
- Let us assume that encryption key(s) and digital certificates are the only thing 'A' and 'B' can exchange in advance.
- Digital certificates are all created by a legitimate CA.

Note: Your secure network application should contain designs only for guaranteeing sender-side non-repudiation (i.e., your design must not include secure design for anything else – this is for simplifying my grading of your work).

Grading policies: Your solution for this question will be graded based on its quality (clearness, technical details, and organized presentations of your ideas).

Please be neat in your hand writing!