CSE 30264
Take Home Final
2014

Student Name John F. Lake, Jr.

- This exam is open book/open note, open web browser.
- This exam is **NOT** open classmate (i.e.: do not discuss this exam or your answers with classmates).
- There are **44** questions covering seven pages (including this sheet) and is worth 200 points.
- Please answer clearly.
- If you provide handwritten answers, please write clearly and cleanly.
- Please be brief and to the point.
- If you find a question ambiguous, be sure to write down any assumptions you make.
- It is better to partially answer a question than to not attempt it at all.

Part I: True/False (2 points each)

The following statements are either True or False.

1) FALSE The root domain name server is a single point of failure.

2) TRUE DNS is a distributed, hierarchical database that only provides host name to IP address mappings.

3) TRUE Every organization with publicly accessible hosts on the Internet must, in some way, provide publicly accessible DNS records that map the host names to IP addresses.

4) TRUE DNS clients who want to prevent TCP SYN flooding attacks should only trust authoritative DNS query responses.

5) FALSE It is standard operation to use ICMP as a transport protocol for user data.

6) FALSE A switch decrements the TTL field in the IP header as packets pass through.

7) TRUE A multiple access protocol is a distributed algorithm that determines how nodes share a channel, i.e., determines when a node can transmit.

8) TRUE Ethernet provides unreliable, connection-less service.

9) FALSE The sockaddr_storage structure was designed specifically for use with file storage systems.

10) FALSE Raw sockets allow the programmer to transmit structures through the network without the need for serialization.

Part II: Short Answer (5 points each)

11) List three types of firewalls, rank them from least secure to most secure, and give a few characteristics of each type of firewall.
-Packet Filtering: This method simply filters IP packets based on a set of rules given.
-Circuit-Proxy: Perform the same job of packet filtering firewalls, but operate up to the transport layer of the OSI stack.
-Application-Proxy: this firewall type looks at the specific applications and has the benefit of understanding protocols such as FTP, DNS, and HTTP.

12) What is the difference between 802.11 independent (ad hoc) BSS mode and infrastructure mode?

Ad hoc mode is peer to peer and is usually temporary, while infrastructure usually involves access points (routers), and is more of a client/server model.

13) What is QoS and how does it relate to over-provisioning?

It is quality of service. It is how well real time applications run over the network. For example, when multimedia applications that are lagging and slow over the network, it is a good indication of poor QoS. Over-provisioning is a cheap way of improving the quality of service by simply expanding the capacity of a network to be able to handle peak traffic loads. Over-provisioning, however, doesn't work with greedy protocols that take up all of the possible bandwidth they can.

14) Compare and contrast how a firewall is related to a NAT.

A firewall is used to block certain traffic based on particular attributes to a particular host. Network Address Translation can prevent hosts outside of your stub domain from connecting to you. You can connect to outside hosts, but they cannot connect to you. They are very similar because they are both used to block traffic, but NAT changes the IP packet headers of IP packets, instead of just blocking them, and isn't as secure as a firewall.

15) A key characteristic of the network is the DBP, the delay-bandwidth product. How does DBP affect the performance of TCP? How does DBP affect the performance of UDP?

DBP affects TCP because TCP is a window-based protocol. You cannot make TCP buffers larger than the DBP size. The higher the DBP, the higher the performance of the network with TCP will be. UDP isn't as affected because it isn't a connection-oriented protocol and doesn't rely on a window, but with a larger DBP it is possible to send more packets (or to send packets faster), so it makes performance better.

16) Name three utilities you might use in order to troubleshoot network connection problems.
Netstat
Traceroute
ipconfig

17) Compare / contrast the following terms: AS, BGP, OSPF, MPLS.

AS: (Autonomous System)- a network or collection of networks managed by a particular group.
BGP: (Border Gateway Protocol)- a routing protocol that can be used for routing within an autonomous system. This routes based on rules set by a network administrator.
OSPF: (Open Shortest Path First)- this is another routing protocol, but is an interior protocol used within autonomous systems, rather than an external protocol like BGP.
MPLS: (Multiprotocol Label Switching) – a protocol-independent transport that transports data based on short path labels. This can be used in conjunction with BGP and OSPF, as it is protocol-independent.

18) Compare / contrast the following compression methods and explain which are lossy/lossless.
a) JPEG: this is a lossy compression technique and is used for digital images. The degree of compression can be adjusted.
b) Lempel-Ziv: this is a group of lossless compression techniques. They are essentially dictionary encoders, and have helped develop other compression techniques such as GIF and PNG.
c) RLE: Run length encoding is a very simple lossless encoding technique used to encode data. This simply looks at sequences of characters and replaces them with a number and a letter for the character in the sequence. JPEG utilizes RLE for some of its operations.
d) MPEG: this is a lossy compression for video and audio. It was extended from JPEG, and is used very frequently all over the world. MP3 is a version of MPEG.

19) ARP and DNS both depend on caches; ARP cache entry lifetimes are typically less than 10 minutes, while DNS cache is on the order of days. Justify this difference. What undesirable consequences might there be in having too long a DNS cache entry lifetime?

ARP doesn't need a very long timeout because it is used for very temporary connections that are going to change quickly. DNS can justify a longer timeout because URL locations won't change as often. If the DNS cache had a longer timeout, it could be possible that a website moved locations but wasn't updated in the cache, so a client would not be able to properly access it.

20) You are in a Skype conversation with a colleague in a branch office. The connection becomes jittery and laggy, eventually resuming to normal operation. The colleague makes the remark that the company should make IPv6 a priority to improve the videoconferencing quality. Is this statement correct? Why or why not?

This is incorrect. The difference in quality of service between IPv4 and IPv6 is negligible. They have very similar functions, and IPv6 doesn't offer better QoS just for having more addresses.

21) Describe TCP slow start. Why is it used?

Slow start is used for congestion control. It is a strategy of doubling window size, or number of packets sent out, every time an ACK is received. As soon as a loss occurs, TCP assumes it is because of congestion, and switches to linear growth.

22) Explain the terms additive increase and multiplicative decrease in the context of TCP congestion control.
Additive increase/multiplicative decrease is a feedback control algorithm in TCP and is used for congestion avoidance. Essentially, additive increase means that the congestion window is increasing linearly, and multiplicative decrease means that when a loss occurs, the window is decreased exponentially; it's like you are taking 3 steps forward and 9 steps backward.

23) Explain how TCP flow control works.

TCP uses end-to-end flow control in the form of sliding window flow control, where the receiver tells the sender how much data to send (i.e. the window) without accepting an ACK and a window update. Without this, the sender wouldn't know how much data to send, and some of it would be lost.

24) What are the possible approaches for delivering quality of service guarantees in networked applications?

You could use approaches to target specific applications, such as RSVP (Resource Reservation Protocol), or you could target a large number of applications with something like differentiated services. RSVP reserves resources so that you can guarantee a certain level of QoS for particular applications. If you used this, you would allocate a particular amount of resources for each node along a path, thereby guaranteeing that the application would be able to communicate well.

25) What is the difference between congestion control and flow control?

Flow control is used by the receiving end to let the sender know how much data to send, and when to send it. Sliding window and stop and wait are examples of flow control. This is rather simiple, and just controls the flow of data in one particular connection. Congestion control, on the other hand, looks at many applications running concurrently and determines how to allocate bandwidth so that the link used isn't 'congested' by the different applications. Quality of service is one thing that can be affected by a lack of congestion control.

Part III: Problem Solving (Points as marked)

26. **(10 points)** Below are the first 60 bytes of a TCP/IP packet captured using Ethereal on an Ethernet network. Decode the packet for the following fields:
- (2 pts) Ethernet MAC source and destination addresses (hexadecimal)
- (2 pts) IP source and destination addresses (in standard dotted-decimal format)
- (2 pts) TCP source and destination port numbers (decimal)
- (2 pts) Type of TCP segment (e.g., SYN, FIN, ACK, etc.)
- (2 pts) Application layer protocol (and command, if applicable)

```
08 00 20 f7 88 7d 00 11 43 b7 92 43 08 00 45 00  ....}..C..C..E.
02 4b 1f f8 40 00 80 06 ca 9b 83 f7 03 2a 83 f7 .K..@.......*..
03 01 08 68 00 50 e0 5a 79 da 38 0b ef 53 50 18 ...h.P.Zy.8..SP.
ff ff 80 d7 00 00 47 45 54 20 2f 7e 63 68 72 69 ......GET /~chri
73 74 65 6e 2f 63 68 72 69 73 74 65 6e 2e 68 74 sten/christen.ht
6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 ml HTTP/1.1..Hos
```

Mac source:	**00:11:43:b7:92:43**
Mac destination:	**08:00:20:f7:88:7d**
IP source:	**131.247.3.42**
IP destination:	**131.247.3.1**
TCP source port**:**	**2152**
TCP source destination:	**80**
Type of TCP segment:	**PSH, SYN, and FIN**
App Layer Protocol:	**HTTP with the GET command**

27. **(5 points)** Your Internet service provider supplies one public IP address with your subscription. You and your roommates have a total of six computers. Describe what hardware / software / techniques would be required for all six computers to be able to communicate on the Internet simultaneously.

Not every computer has an IP address; you would use a router to connect all of the devices to the Internet. All of the 6 computers would have a local address, not seen by external hosts, and the router would forward information to them based on their specific local address on that IP address. If one of them wanted to use a web browser, for example, he would send a packet to the router, the router would take care of retrieving the HTTP request, and then the router would send the packet back to the local address that requested it.

28. **(5 points)** For the local network (LAN) in problem 27, identify and describe at least 5 protocols that impact the communications of nodes on the network.

IP: There is one IP address that needs to connect the router to the internet and actually get data.
DHCP: Protocol to give users local addresses from the router.
TCP: Used to actually send data from my computer through the router to the internet.
RSVP: Used for QoS to ensure proper distribution of resources among the users.
MAC: Used in combination with DHCP; unique address of users on the local scale.

29. **(5 points)** Given an IP address: 150.192.128.27 with a netmask 255.255.224.0 answer the following: What class network does this address come from? Identify the class 'X' network ID and all feasible subnetworks (e.g. 150.192.128.0 is one of them) associated with the network assuming all of the subnetworks use the same netmask?

This comes from class B. The class B network ID is 150.192.128.0. There are 8190 usable subnetworks, from 150.192.128.1 to 150.192.159.254.

30. **(10 points)** Place the following steps of a remote procedure call into the right order.
A. Client's OS gives message to client stub.
B. Server stub unpacks parameters, calls server.
C. Client procedure calls client stub in normal way.
D. Remote OS gives message to server stub.
E. Server's OS sends message to client's OS.
F. Client stub builds message, calls local OS.
G. Stub unpacks result, returns to client.
H. Server stub packs it in message, calls local OS.
I. Server does work, returns result to the stub.
K. Client's OS sends message to remote OS.

In order from start to finish: C F K D B I H E A G

31. **(5 points)** Suppose that a receiver, in its effort to control the bursts from the transmitter, delays sending ACKs until the receiver has enough empty buffers. What is a possible problem with such a strategy? How can the problem be resolved?

A problem with this is the fact that there might be a timeout if the receiver waits for too long. You can't assume that you will have the time to wait for empty buffers. Increasing the buffer size on the receiving end and queuing packets into the buffers can resolve this problem.

32. **(5 points)** Briefly describe how the traceroute tool works (i.e., how does it identify the routers that make up an Internet path).

Traceroute sends an IP packet with increasing TTL values. When it sends the first packet, the TTL value is set to 1. This gives the address of the first router. When the TTL field is 2, it will get the second router. Traceroute will continue this until it receives a "port unreachable" ICMP message, which means that the TTL was large enough for the packet to reach the destination. All of the routers that were observed in the meantime were the ones that made up the internet path.

33. **(10 points)** Suppose we could deploy a mechanism that would ensure IP source addresses correspond to the actual sender of a packet (i.e., it's impossible to "spoof" source addresses). For each of the following threats, explain whether (and briefly why) the mechanism would: (i) completely eliminate the threat, (ii) eliminate some instances of the threat, but not all of them, or (iii) have no impact on the threat.

(a) Buffer overflow attacks
There would be no impact on the threat, as buffer overflow attacks can be performed regardless of one's IP address. Buffer overflow attacks involve choosing certain fields in a header or address and exploiting the buffer size.

(b) TCP SYN flooding
This threat would be completely eliminated, as it relies completely on spoofing IP addresses.

(c) Phishing Attacks
It would eliminate the threats that use spoofed addresses to send emails, but there are other ways of phishing that don't require address spoofing.

(d) Spam email
This would have little impact on the threat because most spam email is just from business. There might be some emails from IP address sources that might be spoofed and might claim to be someone else, but they would fall more under the phishing attack category.

(e) Port Scans
There would be no affect on this, as you can do a port scan from any address.

34. **(25 points)** Attached are server.c and client.c with some "bugs". Identify the bugs and explain how to fix them. (there are at least 14 errors between the two files. **Ignore missing return value checks**).

```
1.  //================== file = server.c =====================
2.  #include <stdio.h>
3.  #include <string.h>
        //BUG: no include for <sys/socket.h> or <sys/types.h>
4.  #include <windows.h>
5.  #define PORT_NUM 1050 // Arbitrary port number for the server
6.  void main(void) {
7.      unsigned int welcome_s;
8.      struct sockaddr_in server_addr;
9.      unsigned int connect_s;
10.     struct sockaddr_in client_addr;
```

```
11.     struct in_addr client_ip_addr;
12.     int addr_len;
13.     char out_buf[100];
14.     char in_buf[100];
15.     server_addr.sin_family = AF_INET;
16.     server_addr.sin_port = PORT_NUM;
17.     server_addr.sin_addr.s_addr = htonl(INADDR_ANY);
          //BUG: you are using htonl but you aren't sending it across the network! Should be a function to get
          the IP address from INADDR_ANY.
          //BUG: You never make a call to socket(), so welcome_s doesn't have a socket!!!
// Listen on welcome socket for a connection
18.     listen(welcome_s, 0);
          //BUG: You don't listen in UDP!!!
// Accept a connection.
19.     connect_s = accept(welcome_s, (struct sockaddr *)&client_addr, &addr_len);
          //BUG: You don't connect either! UDP is connectionless!
20.     printf("Accept completed \n");
// Send to the client using the connect socket
21.     strcpy(out_buf, "Test message from server to client");
22.     send(welcome_s, out_buf, strlen(out_buf), 0);
        //BUG: Should be strlen(out_buf)+1 to account for null terminator.
// Receive from the client using the connect socket
23.     recv(welcome_s, in_buf, sizeof(in_buf), 0);
24.     printf("Received from client... data = '%s' \n", in_buf);
// Close sockets and clean-up
25.     closesocket(connect_s);
          //BUG: correct call is close(connect_s);
26. }
```

```
1.  //========================== file = client.c ==============================
2.  #include <stdio.h>
3.  #include <string.h>
    //BUG: no include for <sys/socket.h> or <sys/types.h>
4.  #include <windows.h>
5.  #define PORT_NUM 1050         // Port number used at the server
6.  #define IP_ADDR "127.0.0.1"  // IP address of server (*** HARDWIRED ***)
7.  void main(void)  {
8.      unsigned int client_s;
9.      double server_addr;
          //BUG: Need struct sockaddr_in or addrinfo; can't store all of the address info with a double.
10.     char out_buf[10];
11.     char in_buf[10];
// Create a client socket
12.     client_s = socket(AF_INET, DATAGRAM, 0);
          //BUG: DATAGRAM should be SOCK_DGRAM
// Fill-in the server's address information and connect with the listening server
13.     server_addr.sin_family = AF_INET;
14.     server_addr.sin_port = PORT_NUM;
15.     server_addr.sin_addr.s_addr = inet_addr(IP_ADDR);
          //BUG: server_addr is NOT A STRUCT.  You need to use addrinfo or sockaddr_in
16.     connect(client_s, (struct sockaddr *)&server_addr, sizeof(server_addr));
          //BUG: You don't connect with UDP!!!
// Receive from the server using the client socket
17.     recv(client_s, in_buf, sizeof(in_buf), 0);
18. printf("Received from server... data = '%s' \n", in_buf);
// Send to the server using the client socket
19.     strcpy(out_buf, "Test message from client to server");
20.     send(client_s, out_buf, strlen(out_buf), 0);
        //BUG: Should be strlen(out_buf)+1 to account for null terminator.
```

```
// Close and clean-up
21.     closesocket(client_s);
          //BUG: Correct Call is close(client_s);
22. }
```

Part IV: Multiple Choice: (3 points each)

35) Suppose application A is using a UDP socket to transfer data to application B on a remote host. Suppose application A calls send() on the given socket 10 times. Is it possible for the underlying network stack to transmit **more** than 10 data frames?

(a) -> Yes, connection setup frames will be sent in addition to data frames.
(b) No, the application will send exactly 10 data frames.
(c) Both of the above statements are true.
(d) Not enough information given to answer the question.

36) Suppose application A is using a UDP socket to transfer data to application B on a remote host. Suppose application A calls send() on the given socket 10 times. Is it possible for the underlying network stack to transmit **fewer** than 10 data frames?

(a) Yes, the network stack can combine multiple writes into a single frame.
(b) -> No, the application will send exactly 10 data frames.
(c) Neither of the above statements are true.
(d) Not enough information given to answer the question.

37) Linux traceroute expects to receive an ICMP _____ packet when the probe reaches the destination host.

(a) Time Exceeded
(b) Network Administratively Prohibited
(c) Echo Request
(d) -> port unreachable

38) When the hop-count field in an IP packet reaches zero and the destination has not been reached, an ICMP _____ error message is sent back to the sending machine.

(a) destination-unreachable
(b) -> time-exceeded
(c) parameter-problem
(d) none of the above

39) The _____ utility allows you to query the DNS database from any computer on the network and find the host name of a device by specifying its IP address, or vice versa?

(a) ipconfig
(b) tracert
(c) -> nslookup
(d) netstat

Part V: Course Evaluation (2 points each)

You will receive full credit for this question regardless of how you respond, so **DO NOT ANSWER IT UNTIL YOU ARE FINISHED** with the remainder of the exam. There is no penalty if you don't get to it.

40) What topic covered in this course did you find the most interesting?
I found socket programming to be the most interesting.

41) What topic did you find least interesting, and why?
Probably resource allocation & congestion; it seemed very dry and tedious.

42) How long did you spend on each project? Which project did you prefer?
It varied, but I spent between 10 and 20 hours per project & program. My favorite program was the RPC one.

43) Was there a networking topic you wish we had covered?
I honestly don't know enough about networking to know what I would have wanted to study.

44) Is there anything you'd suggest be done differently the next time this course is offered?
I would have more programming assignments, but I would make each of them simpler. The infrequent large projects sometimes were overwhelming and covered many different topics simultaneously.