Name ..... ID ..... Section ..... Seat No .....

Sirindhorn International Institute of Technology
Thammasat University

Final Exam Answers: Semester 2, 2011

Course Title: ITS332 Information Technology Laboratory II

Instructor: Steven Gordon

Date/Time: Tuesday 3 April 2012; 9:00–12:00

Instructions:

- This examination paper has 21 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).
- Assume the user in all questions has administrator privileges (that is, you can ignore the need for `sudo`).
- Reference material at the end of the exam may be used.

Question 1 [24 marks]

In this question assume you only have access to a Ubuntu Linux terminal (there are no graphical applications available). You must write the command, including necessary options, to complete the task. You do not need to give `sudo` in your answers (even if the command requires it). Your answer must be just one command—you cannot use two or more commands for a single answer. Assume the computer you are executing the commands on has one LAN card, `eth0`, with IP address 1.2.3.4 and subnet 255.255.255.0. All questions are worth 1.5 marks. *SG Update: The question parts are independent, e.g. your answer in part (a) does not change the scenario described above when answering part (b).*

(a) Capture up to 1500 Bytes of all packets sent/received across the network, saving the output in the file `output.cap`.

Answer. *`tcpdump -i eth0 -s 1500 -w output.cap`*

(b) Display the current routing table on your computer.

Answer. *`route`*

(c) Change the IP address of your LAN card to `1.2.3.5`.

Answer. *`ifconfig eth0 1.2.3.5 netmask 255.255.255.0`*

(d) Send 5 ICMP echo request packets to computer with address `1.2.3.1` at a rate of 4 per second.

Answer. *`ping -c 5 -i 0.25 1.2.3.1`*

(e) Obtain or renew an IP address lease from a server.

Answer. *`dhclient`*

(f) Edit the file `/etc/hosts` in a text editor.

Answer. *`nano /etc/hosts`*

(g) Display the interfaces on your computer.

Answer. *`ifconfig`*

(h) Set the default router for your computer to be `1.2.3.1`.

Answer. *`route add default gw 1.2.3.1`*

(i) Block other computers from sending packets to the web server on your computer.

Answer. *iptables -A INPUT -p tcp --dport 80 -j DROP*

(j) Restart the web server on your computer.

Answer. *apache2ctl restart*

(k) Login to the computer `1.2.3.6` so you can execute commands on that computer.

Answer. *ssh 1.2.3.6*

(l) Compile the C program `myserver.c` to produce the executable `serv1`.

Answer. *gcc -o serv1 myserver.c*

(m) View the set of routers between your computer and the Facebook web server.

Answer. *tracepath www.facebook.com*

(n) View the current set of TCP connections that your computer has open.

Answer. *netstat -t*

(o) Download the `/its332/exam.html` file from the web server on Steve's computer with IP address `9.8.7.6`.

Answer. *wget http://9.8.7.6/its332/exam.html*

(p) Start a TCP server that listens on port 5432.

Answer. *nc -l 5432*

Question 2 [5 marks]

In this question assume you only have access to a Ubuntu Linux terminal (there are no graphical applications available). You must give the file name to view or edit to complete the task. You do not need to give the full path (the directory); just give the name of the file. All questions are worth 1 mark.

(a) View the default DNS server that your computer uses.

Answer. */etc/resolv.conf*

(b) View the port number used by an NTP server (a NTP server is used for synchronising clocks network across a network)

Answer. */etc/services*

(c) Change the computer from a host to router.

Answer. */proc/sys/net/ipv4/ip_forward*

(d) View the time remaining for using the current dynamically allocated IP address.

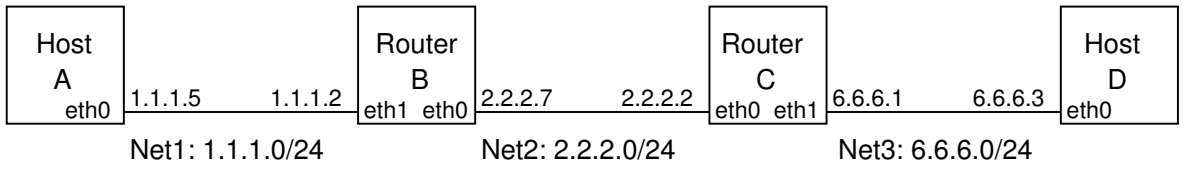
Answer. */var/lib/dhcp3/dhclient.leases*

(e) Change the base directory used by the web server on your computer (i.e. change the location where the web server stores files it offers).

Answer. */etc/apache2/sites-available/default*

Question 3 [7 marks]

Consider the network design diagram below.



Dest	Next
Net1	direct
*	B

Dest	Next
Net1	direct
Net2	direct
*	C

Dest	Next
Net1	B
Net2	direct
Net3	direct

Dest	Next
Net1	C
Net2	C
Net3	direct

(a) Write the command to set the IP address on D. [2 marks]

Answer. *ifconfig eth0 6.6.6.3 netmask 255.255.255.0*

(b) Write the command to add the 1st row to the routing table for C. [2 marks]

Answer. *route add 1.1.1.0 netmask 255.255.255.0 gw 2.2.27 dev eth0*

(c) Write the command(s) to configure the `iptables` firewall on B to block all pings to/from any host on network `6.6.6.0`. Even though there is only one host shown in each network, assume that there may be many more. Also assume that the default policy is ACCEPT). [2 marks]

Answer. *iptables -A FORWARD -p icmp -d 6.6.6.0/24 -j DROP*

The single command will stop ping from working (and is correct). But to stop the requests so that hosts within `1.1.1.0` never receive a request you could also add: *iptables -A FORWARD -p icmp -s 6.6.6.0/24 -j DROP*

(d) What type of Ethernet cable should you use to connect B to C? [1 mark]

Answer. *Cross-over cable*

Question 4 [9 marks]

Assume Apache web server has been correctly configured and is running on a computer with IP address `72.16.4.3` and domain name `www.example.com`. For reference, a portion of the configuration file `/etc/apache2/sites-available/default` is given below.

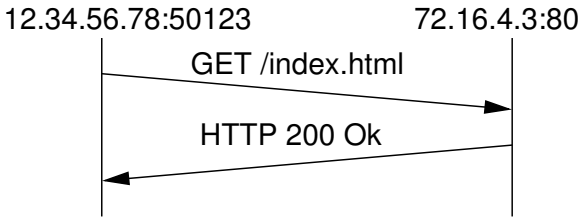
```
<VirtualHost *:80>
ServerName www.example.com
ServerAdmin webmaster@example.com

DocumentRoot /var/www
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/>
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
</Directory>
... (rest of text hidden by Steve)
```

Selected files and directories on this computer are:

```
/home/user/
/home/user/web/
/home/user/web/test.html
/etc/apache2/
/etc/apache2/apache2.conf
/etc/apache2/sites-available/
/etc/apache2/sites-available/default
/etc/apache2/passwords.txt
/var/www/
/var/www/index.html
/var/www/contact.html
/var/www/about.html
/var/www/images/
/var/www/images/photo.jpg
/var/www/myfiles/
/var/www/myfiles/questions.html
/var/www/myfiles/answers.html
```

Answer the following questions based on the above information.

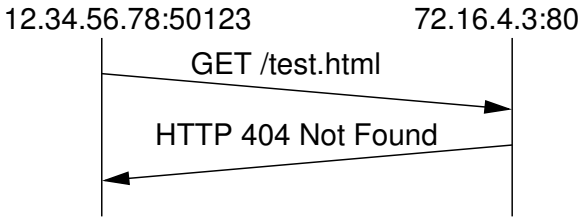
(a) A user of a web browser on computer `12.34.56.78` enters the following address into the browser: `http://www.example.com/index.html`. Draw a message sequence diagram that illustrates the exchange of HTTP messages. You must clearly show the information included in the request, as well as the status code include in the response. Assume no caching is used. [1.5 marks]



(b) If the web browser is using port 50123, then complete the fields of the following headers for the first packet in the above exchange of HTTP messages. [1.5 marks]

- IP Source address: *12.34.56.78*
- IP Destination address: *72.16.4.3*
- IP Protocol number: *6*
- TCP Source port: *50123*
- TCP Destination port: *80*

(c) Assume the user of the web browser now clicks on a link with the following URL: `http://www.example.com/test.html`. Draw a message sequence diagram. [2 marks]



Assume now additional information is added to the Apache configuration file (and once correctly configured, Apache is restarted):

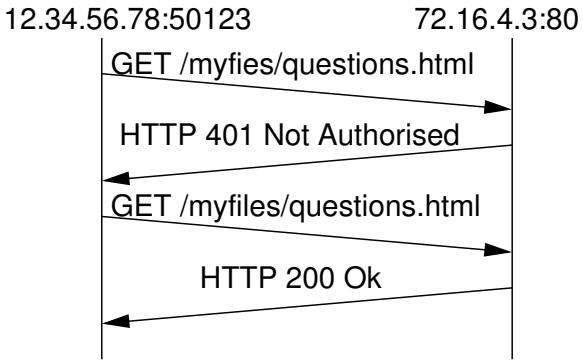
```
<Directory "/var/www/myfiles">
   AuthType Basic
   AuthName "Questions and answers"
   AuthUserFile /etc/apache2/passwords.txt
   Require user steve
</Directory>
```

(d) Explain what the following command does? [1 mark]

```
$ sudo htpasswd /etc/apache2/passwords.txt steve -b mysecret
```

Answer. *Adds the user* steve *and the corresponding password* `mysecret` *to the passwords file (*`passwords.txt`*).*

(e) Assume the user of the web browser now enters the following URL into the address bar: `http://www.example.com/myfiles/questions.html`. Draw a message sequence diagram. [2 marks]



(f) In the above message sequence diagram, in which message/packet is the password inside? [1 mark]

Answer. *The third message.*

Question 5 [11 marks]

Consider the commands and output recorded on a Ubuntu Linux terminal by user *sgordon*. Some commands/outputs have been replaced by variables (a)—(k).

```
$ cd
$ pwd
(a)
$ ls -l
total 0
$ (b)
$ cd exam
$ echo "hello" > message.txt
$ cat message.txt
(c)
$ cp /etc/services (d)
$ cp message.txt (e)
$ (f)
total 28
-rw-rw-r-- 1 sgordon sgordon     6 2012-03-22 14:45 another.txt
-rw-rw-r-- 1 sgordon sgordon     6 2012-03-22 14:44 message.txt
-rw-r--r-- 1 sgordon sgordon 19666 2012-03-22 14:45 services
$ echo "its steve" >> another.txt
$ wc message.txt
1 1 6 message.txt
$ wc another.txt
 (g)  (h) (i) another.txt
$ wc services
  599  2701 19666 services
$ ls -l *.txt
-rw-rw-r-- 1 sgordon sgordon 16 2012-03-22 14:47 another.txt
-rw-rw-r-- 1 sgordon sgordon  6 2012-03-22 14:44 message.txt
$ (j)
$ ls -l *.txt
-rw-rw-r-- 1 sgordon sgordon  6 2012-03-22 14:44 message.txt
-rw-rw-r-- 1 sgordon sgordon 16 2012-03-22 14:47 third.txt
$ (k)
$ ls
message.txt  third.txt
```

Write the commands/outputs for the variables (a)—(k) below. Each part is worth 1 mark.

(a) `/home/sgordon`

(b) `mkdir exam`

(c) `hello`

(d) `.`

(e) `another.txt`

(f) `ls -l`

(g) `2`

(h) `3`

(i) `16`

(j) `mv another.txt third.txt`

(k) `rm services`

Question 6 [6 marks]

The following shows portion of an example log from Apache web server running on the computer with domain name `www.example.com`. Assume no firewalls or proxies in the network.

```
61.19.242.176 - - [05/Dec/2010:08:21:52 +0700] "GET /index.html HTTP/1.1"
 200 1200 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:21:53 +0700] "GET /css/main.css
HTTP/1.1" 200 540 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:21:59 +0700] "GET /about/contact.html
HTTP/1.1" 200 906 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:22:30 +0700] "GET /exams/midterm.html
HTTP/1.1" 200 906 "http://www.example.com/about/contact.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:05 +0700] "GET /files/answers.txt
HTTP/1.1" 200 1100 "http://sandilands.info/exams/midterm.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:21 +0700] "GET /index.html HTTP/1.1"
304 20 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:21 +0700] "GET /css/main.css
HTTP/1.1" 304 20 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:45 +0700] "GET
/lectures/handouts.html HTTP/1.1" 200 1330
"http://www.example.com/index.html" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:54 +0700] "GET /lectures/topic2.html
HTTP/1.1" 404 320 "http://www.example.com/lectures/handouts.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"
```

```
61.19.242.176 - - [05/Dec/2010:08:24:22 +0700] "GET /lectures/topic1.html
HTTP/1.1" 200 2303 "http://www.example.com/lectures/handouts.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"
```

Answer the following questions based on the above information.

(a) How many bytes in the file `/css/main.css`? [1 mark]

Answer. *540 Bytes*

(b) What protocol version is used by the web browser to retrieve the web pages? [1 mark]

Answer. *v1.1*

(c) Which file(s) was requested but does not exist on the server? [1 mark]

Answer. */lectures/topic2.html*

(d) There are two requests for `/index.html` in the log. The requests result in different responses. What is an advantage of the 2nd response (compared to the 1st)? [1.5 marks]

Answer. *The first response is 200 Ok and includes the web page; the second response is 304 Not Modified and doesn't include the web page. The advantage of the 2nd response is that less data is sent across the network (faster data delivery).*

(e) What is an disadvantage of the 2nd response (compared to the 1st)? [1.5 marks]

Answer. *The disadvantage of the 2nd response is that the page used by the browser may be out-of-date (compared to the page on the web server)*

Question 7 [5 marks]

You are running Ubuntu Linux on your home computer. Installed is Apache Web Server, which you use only for testing. That is, you only access the web server on your computer from localhost (`127.0.0.1`). You want to prevent everyone on the Internet from accessing your web server. Of course, you still want to allow your own computer to access web servers and other servers (email, instant messaging, ssh, ...) on the Internet. You use `iptables` as the firewall on your computer (there are no other firewalls or network address translation in your network). Assume the default firewall policy is ACCEPT.

(a) Give the exact `iptables` command(s) to create the desired firewall. Explain any assumptions. [2.5 marks]

Answer. *`iptables -A INPUT -p tcp --dport 80 -i eth0 -j DROP` This assumes eth0 is the LAN interface.*

Now assume you want to prevent everyone on the Internet from accessing any server running on your computer (instead of just the web server).

(b) Give the exact `iptables` command(s) to create the desired firewall. Explain any assumptions. [2.5 marks]

Answer. *`iptables -A INPUT -p tcp --dport 1:1024 -i eth0 -j DROP` This assumes only servers use ports from 1 to 1024; clients use higher ports*

Question 8 [9 marks]

Consider the two packets below, captured and displayed using tcpdump/Wireshark (other captured packets are not shown). The relevant details of each of the packets is shown on the subsequent pages. Answer the following questions based on this information.

```
No. Time      Source    Destination     Protocol Info
48  5.316001  0.0.0.0   255.255.255.255 DHCP     DHCP Request
50  5.318745  10.10.1.1 10.10.1.198     DHCP     DHCP ACK
```

(a) Explain which computer(s) receive packet number 48. (*Don't* just give the destination address above) [1 mark]

Answer. *All computers on the LAN*

(b) Explain which computer(s) receive packet number 50. (*Don't* just give the destination address above) [1 mark]

Answer. *The computer that sent packet 48 (MAC=`00:17:31:5a:e5:89`).*

(c) What is the port number used by a DHCP client? [1 mark]

Answer. *68*

(d) What is the MAC address of the computer that sent packet number 48? [1 mark]

Answer. *`00:17:31:5a:e5:89`*

(e) After the above two packets have been exchanged, what is the IP address of the computer that sent packet number 48? [1 mark]

Answer. *`10.10.1.198`*

(f) For how long is the computer allowed to use the IP address in part (e)? [1 mark]

Answer. *3 days*

(g) Draw the packet structure for packet number 50, indicating the protocols used and size of each header/data in bytes (Hint: UDP header is 8 Bytes; DHCP is called "Bootstrap" in Wireshark). [3 marks]

Answer. *Ethernet (14) — IP (20) — UDP (8) — Bootp/DHCP (300)*

```
Frame 48 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff
    Source: 00:17:31:5a:e5:89
    Type: IP (0x0800)
Internet Protocol, Src: 0.0.0.0, Dst: 255.255.255.255
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10
    Total Length: 328
    Identification: 0x0000 (0)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0x3996 [correct]
    Source: 0.0.0.0
    Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source port: 68
    Destination port: 67
    Length: 308
    Checksum: 0x0d4d [correct]
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x1a5bb57c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:17:31:5a:e5:89
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option: (t=53,l=1) DHCP Message Type = DHCP Request
    Option: (t=54,l=4) DHCP Server Identifier = 10.10.1.1
    Option: (t=50,l=4) Requested IP Address = 10.10.1.198
    Option: (t=12,l=6) Host Name = "ginger"
    Option: (t=55,l=13) Parameter Request List
    End Option
    Padding
```

```
Frame 50 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45, Dst: 00:17:31:5a:e5:89
    Destination: 00:17:31:5a:e5:89
    Source: 00:50:ba:4c:6b:45
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.1.1, Dst: 10.10.1.198
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10
    Total Length: 328
    Identification: 0x0000 (0)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (0x11)
    Header checksum: 0x92bb [correct]
    Source: 10.10.1.1
    Destination: 10.10.1.198
User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source port: 67
    Destination port: 68
    Length: 308
    Checksum: 0x5d3c [correct]
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x1a5bb57c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.10.1.198
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:17:31:5a:e5:89
    Client hardware address padding: 00000000000000000000
    Magic cookie: (OK)
    Option: (t=53,l=1) DHCP Message Type = DHCP ACK
    Option: (t=54,l=4) DHCP Server Identifier = 10.10.1.1
    Option: (t=51,l=4) IP Address Lease Time = 3 days
    Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    Option: (t=3,l=4) Router = 10.10.1.1
    Option: (t=6,l=8) Domain Name Server = 10.10.10.5
    Option: (t=44,l=8) NetBIOS over TCP/IP Name Server
    End Option
    Padding
```

Question 9 [10 marks]

Consider the C source code in files `file1.c` and `file2.c` in Listings 1 and 2, respectively. They provide similar (but not the same) functionality as the sockets code used in the lab. Note that some error checking code is removed (but they still compile and execute). Answer the questions based on this code.

Listing 1: Source code for file1.c

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4  #include <sys/types.h>
5  #include <sys/socket.h>
6  #include <netinet/in.h>
7  #include <netdb.h>
8  #define MAX_CHAR 1000
9  #define CONST_A 20
10 #define CONST_B 50
11 int main(int argc, char *argv[])
12 {
13         int s, p, n;
14         struct sockaddr_in dst_addr;
15         struct hostent *dst;
16         char d[MAX_CHAR];
17
18         s = socket(AF_INET, SOCK_STREAM, 0);
19         dst = gethostbyname(argv[1]);
20         p = atoi(argv[2]);
21         bzero((char *) &dst_addr, sizeof(dst_addr));
22         dst_addr.sin_family = AF_INET;
23         bcopy((char *)dst->h_addr,
24                 (char *)&dst_addr.sin_addr.s_addr,
25                 dst->h_length);
26         dst_addr.sin_port = htons(p);
27
28         connect(s,(struct sockaddr *) &dst_addr,sizeof(dst_addr));
29         bzero(d,MAX_CHAR);
30         /* fgets also reads the single Enter character '\n' if typed */
31         fgets(d,CONST_A,stdin);
32         n = write(s,d,strlen(d));
33
34         bzero(d,MAX_CHAR);
35         n = read(s,d,CONST_B);
36
37         printf("%s\n",d);
38         return 0;
39 }
```

Listing 2: Source code for file2.c

```
40 #include <stdio.h>
41 #include <string.h>
42 #include <stdlib.h>
43 #include <sys/types.h>
44 #include <sys/socket.h>
45 #include <netinet/in.h>
46 #define MAX_CHAR 1000
47 #define CONST_C 10
48 int main(int argc, char *argv[])
49 {
50         int s, news, p, pid, n;
51         struct sockaddr_in my_addr, src_addr;
52         size_t srcaddrlen;
53         char b[MAX_CHAR], c[MAX_CHAR];
54
55         s = socket(AF_INET, SOCK_STREAM, 0);
56         bzero((char *) &my_addr, sizeof(my_addr));
57         p = atoi(argv[1]);
58         my_addr.sin_family = AF_INET;
59         my_addr.sin_addr.s_addr = INADDR_ANY;
60         my_addr.sin_port = htons(p);
61         bind(s, (struct sockaddr *) &my_addr, sizeof(my_addr));
62         listen(s,5);
63         srcaddrlen = sizeof(src_addr);
64
65         while (1) {
66                 news = accept(s, (struct sockaddr *) &src_addr, &srcaddrlen);
67                 pid = fork();
68                 if (pid == 0)  {
69                         close(s);
70                         bzero(b,MAX_CHAR);
71                         n = read(news,b,CONST_C);
72                         printf("Message: %s\n",b);
73                         sprintf(c,"Data is %s",b);
74                         n = write(news,c,strlen(c));
75                         exit(0);
76                 }
77                 else  {
78                         close(news);
79                 }
80         }
81     return 0;
82 }
```

Assume files `file1.c` and `file2.c` are compiled to produce `program1` and `program2`, respectively. `program2` is started on computer with IP address `3.3.3.3` and using port `5555`. `program1` will be run on a computer with IP address `6.6.6.6`.

(a) *SG Update: the parts were originally numbered from (b) onwards, i.e. (a) was missing.* What command, including arguments, is used to run `program1`? [1 mark]

Answer. *`program1 3.3.3.3 5555`*

Consider now after `program1` is started, the user of the program types in to the terminal: *network*

(c) What is printed at the computer running `program2`? [1 mark]

Answer. *Message: network*

(d) What is printed at the computer running `program1`? [1 mark]

Answer. *Data is network*

(e) How many bytes of data did `program1` send to `program2`? [1 mark]

Answer. *8 bytes. 7 bytes for each letter in* network*, as well as 1 byte for the Enter character*

Now consider that `program1` is started again, but this time the user types in to the terminal: *networklaboratory*

(f) What is printed at the computer running `program2`? [2 marks]

Answer. *Message: networklab*

Now consider that the value of `CONST_B` in `file1.c` is changed from 50 to 9. After recompiling, the user starts `program1` and types into the terminal: *network*

(g) What is printed at the computer running `program1`? [2 marks]

Answer. *Data is n*

You want to change `program1` so that instead of reading what the user types in from the terminal after the program is started, the program takes an extra command line argument that contains a one word message. You delete line 31 from `file1.c`.

(h) Explain what else you need to do to implement the desired functionality. E.g. what code would you add/modify/delete. Refer to the line numbers in your answer. [2 marks]

Answer. *On line 32 change the two occurrences of `d` to be `argv[3]`*

Question 10 [10 marks]

Referring to the code in Listings 1 and 2, give the line number that implements the following functionality. Each part is worth 1 mark. (Give only one line number for each part, although there may be multiple correct answers.)

(a) Waits until TCP data is received from another host. Line: *35, 71*

(b) Returns the process ID of the parent process when a child process is created. Line: *67*

(c) Blocks until a new TCP connection is established. Line: *28, 66*

(d) Associates an IP address with a socket. Line: *61, 28*

(e) Initiates establishment of a TCP connection. Line: *28*

(f) Obtains the address of the host that connected to the server. Line: *66*

(g) Converts a domain name to an IP address. Line: *19*

(h) Returns the number of bytes successfuly sent. Line: *32, 74*

(i) Writes data to standard output. Line: *37, 72*

(j) Converts a string into an integer. Line: *20, 57*

Question 11 [4 marks]

Consider the output from a command. Values have been replaced by the variables *AAA*, *BBB*, *CCC*, *DDD*, *EEE* and *FFF*.

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=5 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=11 ms
64 bytes from 192.168.1.1: icmp_req=3 ttl=64 time=8 ms
64 bytes from 192.168.1.1: icmp_req=4 ttl=64 time=8 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, AAA received, 0% packet loss, time BBBms
rtt min/avg/max/mdev = CCC/DDD/EEE/FFF ms
```

(a) What is the value of [2 marks]:

AAA: *4* CCC: *5* DDD: *8* EEE: *11*

(b) Assuming Ethernet is the Data Link layer protocol, draw the structure of the packets sent by the command that produced the output. [2 marks]

Answer. *Ethernet* | *IP* | *ICMP*

Reference Material

Below is the syntax of commonly used commands. The values that the user must choose are given enclosed in < and >. Optional fields are enclosed in [and]. You may use this information in your answers.

```
ifconfig [<interface>] [up | down]
ifconfig <interface> <ipaddress> netmask <subnetmask>
ping [-c <count>] [-s <packetsize>] [-i <interval>] <destination>
tracepath <destination>
nslookup <domain> [<dnsserver>]
route [-n]
route add -net <netaddress> netmask <subnet> [gw <gateway>] [dev <interface>]
route del -net <netaddress> netmask <subnet> [gw <gateway>] [dev <interface>]
route add default gw <gateway>
arp [-n]
dhclient [<interface>]
tcpdump [-i <interface>] [-s <packetsize>] [-w <file>]
wget <url>
nc <ip> <port>
nc -l <port>
apache2ctl [start | stop | restart]
htpasswd <passwordfile> <username> [-b <password>]
iptables -A <chain> [<options>]
  where <options> include:
   [-s <sourceip>] [-d <destip>] [-i <ininterface>] [-o <outinterface>]
   [-p <protocol>] [--sport <sourceport>] [--dport <destport>]
   [-j <action>]
iptables -D <chain> [<options>]
iptables -L <chain>
iptables -F <chain>
  where <chain> may be: INPUT | OUTPUT | FORWARD
```

Commonly used files and directories are listed below. You may use this information in your answers.

```
/etc/hosts
/etc/resolv.conf
/etc/network/interfaces
/etc/services
/etc/protocols
/var/lib/dhcp3/dhclient.leases
/proc/sys/net/ipv4/ip_forward
/var/www/
/etc/apache2/sites-available/default
```

Port numbers used by common applications include:

20 FTP data transfer

21 FTP connection control

22 SSH, secure remote login

23 TELNET, (unsecure) remote login

25 SMTP, email transfer between servers

53 DNS, domain name lookups

67 DHCP server

80 HTTP, web servers

110 POP3, client access to email

123 NTP, network time

443 HTTPS, web servers with secure access

631 IPP, Internet printing

Protocol numbers for commonly used transport protocols include:

1 ICMP

2 IGMP

6 TCP

17 UDP

33 DCCP

89 OSPF

Status codes and their meaning for common HTTP responses include:

100 Continue Client should continue to sent the request

200 Ok Requested content is included in response

301 Moved Permanently This and all future requests should be redirected to the given URL

304 Not Modified Requested content has not been modified since last access

401 Unauthorized Requested content requires authentication that has not been provided or is incorrect

403 Forbidden Request is ok, but not allowed to access the requested content

404 Not Found Requested content could not be found on server

503 Service Unavailable Requested server is currently unavailable