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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination Answers: Semester 2/2009

Course Title : ITS332 Information Technology II Laboratory

Instructor : Dr Steven Gordon

Date/Time : Tuesday 22 December 2009, 9:00 to 10:30

Instructions:

- This examination paper has 25 pages (including this page).
- Condition of Examination
  Closed book
  No dictionary
  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.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.
- If a question requires an IP address for an answer, then you may select any valid IP address that satisfies all conditions of the question.
- Unless otherwise indicated, IP refers to IPv4.
- Assume 8 bits = 1 Byte; 1000 Bytes = 1KB; 1000KB = 1MB; 1000MB = 1GB; ...

Command Syntax

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>]
ifconfig <interface> <ipaddress> netmask <subnetmask> up
ping [-c <count>] [-s <packetsize>] [-i <interval>] <destination>
tracepath <destination>
nslookup <domain> [<dnsserver>]
route [-n]
route add -net <netaddress> netmask <netmask> [gw <nextrouter>] dev <interface>
route del -net <netaddress> netmask <netmask>
arp [-n]
dhclient
nc -l -p <port>
nc <destination> <port>
```

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

```
/etc/hosts
/etc/resolv.conf
/etc/network/interfaces
/etc/services
/var/lib/dhcp3/dhclient.leases
/proc/sys/net/ipv4/ip_forward
```

Questions [~~86 marks~~ 83 marks]

Question 1 [3 marks]

The following shows the partial contents of a file:

```
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
```

a) What is the name of the file? [1 mark]

Answer

/etc/services

b) What type of addresses are given in this file? [1 mark]

Answer

Port addresses or numbers

c) The whois protocol allows a client to send a query to server to ask who is the owner of a domain name, block of IP addresses or autonomous system. The server responds with the the owner information. If you run a whois client application on computer with IP address 72.16.0.1 and whois server application on 80.2.0.3, then what transport protocol would be used by the applications? [1 mark]

Answer

TCP (from the whois entry, tcp is used).

Question 2 [6 marks]

The following shows interface configuration information for a computer (called *R*). Answer the questions based only on this output.

```
eth0      Link encap:Ethernet  HWaddr 00:17:31:5a:e5:89
          inet addr:10.10.1.110  Bcast:10.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e589/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60312 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36975 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:82269340 (78.4 MB)  TX bytes:2781062 (2.6 MB)

eth1      Link encap:Ethernet  HWaddr 00:17:31:5A:E7:E8
          inet addr:10.10.6.11  Bcast:10.10.6.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e7e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75759 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37816 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:12593354 (12.0 MB)  TX bytes:32730640 (31.2 MB)

eth4      Link encap:Ethernet  HWaddr 00:17:9a:36:f7:65
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe36:f765/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:308380 errors:0 dropped:0 overruns:0 frame:0
          TX packets:353949 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33101632 (31.5 MB)  TX bytes:326555578 (311.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1526 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1526 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:78780 (76.9 KB)  TX bytes:78780 (76.9 KB)
```

a) What command was used to produce this output? [1 mark]

Answer

ifconfig

b) How many Ethernet cards does the computer have currently configured? [1 mark]

Answer

3 (3 interfaces with Ethernet links)

c) Do you think all Ethernet cards are manufactured by the same company? Explain your answer. [1 mark]

Answer

No. The first 6 digits of the MAC address uniquely identify a manufacturer. `eth0` and `eth1` are the same, however `eth4` is different, indicating a different manufacturer.

d) What is one of the IPv6 addresses assigned to R? [1 mark]

Answer

The IPv6 address is the inet6 field. There are three addresses: fe80::217:31ff:fe5a:e589, fe80::217:31ff:fe5a:e7e8 and fe80::217:9aff:fe36:f765

e) Computer R is a router. What is the total number of megabytes that it has received from other hosts and routers? [1 mark]

Answer

121.9MB. The sum of the bytes received on the Ethernet interfaces.

f) What is the average size of a packet transmitted on `eth1`? [1 mark]

Answer

866 Bytes. Total bytes transmitted is 32730640 while the number of packets transmitted is 37816. Therefore the average size is 32730640/37816 = 866 Bytes.

Question 3 [7 marks]

A command was run on a computer with IP address 192.168.1.2. The output of the command is below:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:23:69:3a:f4:7d   C                     eth0
192.168.1.5              ether   00:17:31:5a:e5:89   C                     eth0
192.168.1.12             ether   00:17:31:e7:33:21   C                     eth0
192.168.1.13             ether   00:21:45:55:e5:73   C                     eth0
192.168.1.106            ether   00:17:31:61:c3:c5   C                     eth0
192.168.1.4              ether   00:20:31:bc:8e:90   C                     eth0
```

a) What was the command? [1 mark]

Answer

arp (or arp -n)

b) What is the name of the protocol that the output shows information for? You may give the full name or abbreviation. In addition, explain the purpose of the protocol that the output shows information for. [2 marks]

Answer

ARP is used to find the hardware address given an IP address.

c) From the information in the output, do you know (circle YES or NO): [4 marks]

i. The IP address of the router on the network? YES NO

ii. The hardware address of computer 192.168.1.2? YES NO

iii. The interface label assigned by the operating system on 192.168.1.2? YES NO

iv. The number of computers on the same LAN as 192.168.1.2? YES NO

Answers

i. No. It is impossible to know which devices is a router from the information (a router does not have to have an address 192.168.1.1).

ii. No. The hardware address of other devices are shown – not for 192.168.1.2.

iii. Yes. eth0 is the interface label used.

iv. No. This shows recently contacted computers, not necessarily all computers on the LAN.

Question 4 [9 marks]

The following shows the output of running three consecutive commands (COMMAND1, COMMAND2, COMMAND3) on a computer with IP address 72.16.0.1.

```
sgordon@host:~$ COMMAND1
nameserver 208.67.222.222
nameserver 208.67.220.220

sgordon@host:~$ COMMAND2
Server:            208.67.222.222
Address:  208.67.222.222#53

Non-authoritative answer:
Name:    www.mit.edu
Address: 18.9.22.169

sgordon@ginger:~$ COMMAND3
Server:            bitsy.mit.edu
Address:  18.72.0.3#53

Name:    www.mit.edu
Address: 18.9.22.169
```

a) Give the complete command (including any input arguments) that the user most likely typed. Note that there may be multiple correct answers. [5 marks]

i. COMMAND1: ____

ii. COMMAND2: ____

iii. COMMAND3: ____

Answers

The output of the first command is the contents of /etc/resolv.conf. Hence the command is likely:

cat /etc/resolv.conf

The output of the second command is the answer from a DNS lookup. Since the default name server (from /etc/resolv.conf) is 208.67.222.222, and the response is from the same address, most likely the command was:

nslookup www.mit.edu

The output of the third command is also from nslookup, but now the response is from bitsy.mit.edu. Hence most likely the command was:

nslookup www.mit.edu bitsy.mit.edu

b) The output shows information related to a system/protocol. What is the name of the system/protocol? You may give the full name or abbreviation. In addition, explain the purpose of the system/protocol that the output shows information for. [2 marks]

Answer

DNS is used to find the IP address of the corresponding domain name.

c) If you opened a web browser and typed “18.9.22.169” in the address/location bar, what do you think will be displayed on your web browser? [1 mark]

Answer

The web page of MIT (www.mit.edu)

d) What does the number 53 (following the #) refer to? [1 mark]

Answer

The port number of the DNS server.

Question 5 [19 marks]

You have 3 computers (A, B and C) running a Ubuntu Linux operating system. You want to connect them to create an internet that has two subnets: 3.3.3.0/24 and 4.4.0.0/16. You will have one host in each subnet, and the hosts must be able to communicate with each other, as well as with the router. The following is the current information from each computer:

Computer A

```
eth0      Link encap:Ethernet  HWaddr 00:17:31:5a:e5:01
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e501/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0 B)  TX bytes:0 (0 B)
          Memory:cffe0000-d0000000
```

Computer B

```
eth1      Link encap:Ethernet  HWaddr 00:17:31:5a:e5:02
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e502/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0 B)  TX bytes:0 (0 B)
          Memory:cffe0000-d0000000
```

Computer C

```
eth1      Link encap:Ethernet  HWaddr 00:17:31:5a:e5:03
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e503/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0 B)  TX bytes:0 (0 B)
          Memory:cffe0000-d0000000

eth2      Link encap:Ethernet  HWaddr 00:17:31:5a:e5:04
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e504/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0 B)  TX bytes:0 (0 B)
          Memory:cffe0000-d0000000
```

Explain how to setup the network by answering the following questions. When giving commands for the answers, use the lines provided and where necessary show them in order. You do not need to use all lines provided.

a) How many cables do you need? What type of cables do you need? [1 mark]

Answer

2 x Ethernet unshielded twister pair (e.g. Category 5) cross-over cables.

b) For each computer, show the complete command(s) (including any input arguments) to set the correct IP addresses: [6 marks]

i. Computer A

1. ______________________________

2. ______________________________

3. ______________________________

Answer

ifconfig eth0 3.3.3.1 netmask 255.255.255.0 up

ii. Computer B

1. ______________________________

2. ______________________________

3. ______________________________

Answer

ifconfig eth1 4.4.0.1 netmask 255.255.0.0 up

iii. Computer C

1. ______________________________

2. ______________________________

3. ______________________________

Answer

ifconfig eth1 3.3.3.2 netmask 255.255.255.0 up

ifconfig eth2 4.4.0.2 netmask 255.255.0.0 up

c) Assuming after setting the IP addresses the routing tables for every computer are empty, show the complete command(s) (including any input arguments) to set the correct routing tables: [6 marks]

i. Computer A

1. ______________________________

2. ______________________________

3. ______________________________

4. ______________________________

Answer

route add -net 3.3.3.0 netmask 255.255.255.0 dev eth0

route add -net 4.4.0.0 netmask 255.255.0.0 gw 3.3.3.2 dev eth0

ii. Computer B

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________

Answer

route add -net 4.4.0.0 netmask 255.255.0.0 dev eth1

route add -net 3.3.3.0 netmask 255.255.255.0 gw 4.4.0.2 dev eth1

iii. Computer C

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________

Answer

route add -net 3.3.3.0 netmask 255.255.255.0 dev eth1

route add -net 4.4.0.0 netmask 255.255.0.0 dev eth2

d) Explain what else you need to do (including any commands/files, as well as which computer(s) changes need to be made on) to allow the two hosts to communicate. [2 marks]

Answer

Set Computer C to be a router by putting the value “1” inside the file:

/proc/sys/net/ipv4/ip_forward

e) ping is often used to test the network. What is the highest layer protocol that ping uses? You may give the full name or the abbreviation. [1 mark]

Answer

ICMP: Internet Control Message Protocol

f) The protocol used by ping is sometimes insufficient to test the network. Assuming there are no servers currently running on any computers, show the command(s) (including any input arguments) that you could use to test communications between hosts using a different protocol. Make sure you indicate the correct ordering of the commands and which computer the command is executed on. [3 marks]

1. on computer ___: ____

2. on computer ___: ____

3. on computer ___: ____

4. on computer ___: ____

Answer

[Question not counted, as some sections did not cover nc]

Computer A: nc – l -p 12345

Computer B: nc 3.3.3.1 12345

Then type a message on Computer B (it should appear on Computer A)

Question 6 [5 marks]

The following shows the the contents of a file on different computers (it is the same file name on each computer, but the contents of the file differs):

Computer A, 23.100.2.3:

```
127.0.0.1          localhost
192.168.1.2        localserver
72.16.0.1          stevesserver
72.16.0.1          stevespc
```

Computer B, 72.16.0.1:

```
127.0.0.1          localhost
131.0.4.1          webserver
72.16.0.1          mycomp
41.16.3.2          localserver
```

Computer C, 131.0.4.1:

```
127.0.0.1          localhost
23.100.2.3         webserver
```

a) What is the name of the file shown? [1 mark]

Answer

/etc/hosts

b) Assuming each computer is attached to the Internet, but there are no DNS servers available, for each of the following commands, will the `ping` be successful? If yes, explain which computer (A, B or C) will receive the `ping`. If no, explain why. [4 marks]

i. Computer A: `ping webserver`

Answer

No. There is no hostname webserver in the hosts file of Computer A.

ii. Computer B: `ping webserver`

Answer

Yes. Computer C will be the destination (matches the hostname webserver).

iii. Computer C: `ping localhost`

Answer

Yes. Computer C will be the destination (ping itself)

iv. Computer A: `ping stevespc`

Answer

Yes. Computer B is the destination.

Question 7 [6 marks]

The following shows output from a `ping` command on the computer *C*. Answer the questions based only on this output.

```
sgordon@basil:~$ ping -c 6 -i 2 www.siit.tu.ac.th
PING www.siit.tu.ac.th (203.131.209.77) 56(84) bytes of data.
64 bytes from 203.131.209.77: icmp_seq=1 ttl=60 time=200.0 ms
64 bytes from 203.131.209.77: icmp_seq=2 ttl=60 time=210.0 ms
64 bytes from 203.131.209.77: icmp_seq=3 ttl=60 time=230.0 ms
64 bytes from 203.131.209.77: icmp_seq=4 ttl=60 time=190.0 ms
64 bytes from 203.131.209.77: icmp_seq=5 ttl=60 time=210.0 ms
64 bytes from 203.131.209.77: icmp_seq=6 ttl=60 time=220.0 ms

--- www.siit.tu.ac.th ping statistics ---

_____ packets transmitted, _____ received, _____% packet loss, time ______ ms

rtt min/avg/max/mdev = _______/_______/_______/_______ ms
```

a) Fill in the 8 spaces in the `ping` statistics. For times, give your answer to the nearest 1 ms (for example, “200ms”). [0.5 marks for each answer].

Answer

The -c option in the command line indicates the number of packets to be transmitted (6). There are 6 packets received from 203.131.209.77, meaning 0% packet loss. The minimum (190), average (210), maximum (230) and deviation (20) of the 6 times can be calculated. The total time to send 6 packets with an interval of 2 seconds (-i option) is 10000ms.

b) How many routers do you think are between the computer *C* and `www.siit.tu.ac.th`? Explain your answer. [2 marks]

Answer

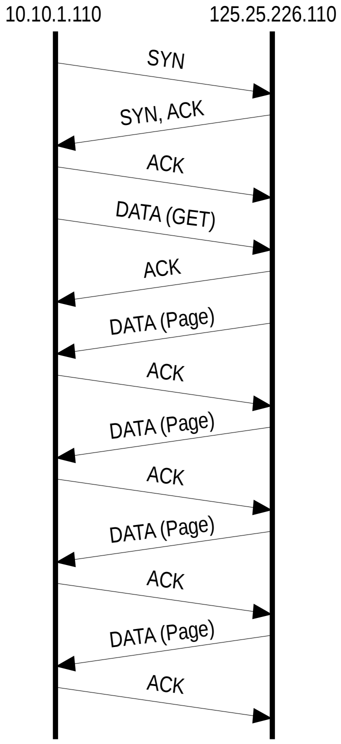
4 routers. If you assume the ping response is sent with time-to-live (TTL) initially 64, then it is decreased by one by each router. Therefore the packet must pass via 4 routers to be received with a value of 60. (Although it is not practical, you may assume other initial values, such as 255).

Question 8 [12 marks]

The following pages show the text output from a packet capture in Wireshark. Answer the questions based only on this output.

a) Draw a diagram that illustrates all TCP segments in the connection setup and data transfer for the TCP connection used to transfer the first web page. Make sure you clearly label the message types (or other identifying information). (Hint: only draw the segments belonging to the one TCP connection) [5 marks]

Answer



b) What is the address of 10.10.1.110's DNS server? [1 mark]

Answer

10.10.10.9. Because the first packet is a DNS query sent from 10.10.1.110 to 10.10.10.9.

c) The contents of the file `www.sandilands.info/siit/index.html` is contained in which packets (give the packet number from the capture)? [1 mark]

Answer

8, 10, 17, 19.

d) There are multiple port numbers shown in the capture. List all port numbers, and explain what application uses them. [2 marks]

Answer

80. Used by web server.

49185, 49186. Used by web browser (client).

e) In the set of packets captured, is the content of the file `www.sandilands.info/siit/css/site.css` sent? Explain how you know the answer. [1 mark]

Answer

Yes. Packet 21 shows the 200 Ok response, meaning the file was sent from server to client.

f) In the set of packets captured, is the content of the file `www.sandilands.info/favicon.ico` sent? Explain how you know the answer. [1 mark]

Answer

No. Packet 26 shows 304 Not Modified meaning the file was not set during this transfer – it has been previously.

g) What is the MAC address of the computer using the web browser in this exchange? [1 mark]

Answer

00:17:31:5a:e5:89

The text output from Wireshark:

```
No. Time      Source          Destination     Prot. Info
 1  0.000000  10.10.1.110     10.10.10.9      DNS   Standard query A www.sandilands.info
 2  0.219620  10.10.10.9      10.10.1.110     DNS   Stand. query resp. CNAME sandilands.info A 125.25.226.110
 3  0.219861  10.10.1.110     125.25.226.110  TCP   49185 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
 4  0.220618  125.25.226.110  10.10.1.110     TCP   80 > 49185 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
 5  0.220646  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
 6  0.220682  10.10.1.110     125.25.226.110  HTTP  GET /siit/index.html HTTP/1.1
 7  0.221617  125.25.226.110  10.10.1.110     TCP   80 > 49185 [ACK] Seq=1 Ack=403 Win=6912 Len=0
 8  0.483472  125.25.226.110  10.10.1.110     TCP   [TCP segment of a reassembled PDU]
 9  0.483494  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=403 Ack=1449 Win=8768 Len=0
10  0.483501  125.25.226.110  10.10.1.110     TCP   [TCP segment of a reassembled PDU]
11  0.483509  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=403 Ack=1526 Win=8768 Len=0
12  0.494431  10.10.1.110     125.25.226.110  TCP   49186 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
13  0.495468  125.25.226.110  10.10.1.110     TCP   80 > 49186 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
14  0.495486  10.10.1.110     125.25.226.110  TCP   49186 > 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
15  0.495525  10.10.1.110     125.25.226.110  HTTP  GET /siit/css/site.css HTTP/1.1
16  0.496470  125.25.226.110  10.10.1.110     TCP   80 > 49186 [ACK] Seq=1 Ack=413 Win=6912 Len=0
17  0.510461  125.25.226.110  10.10.1.110     TCP   [TCP segment of a reassembled PDU]
18  0.510477  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=403 Ack=2934 Win=11648 Len=0
19  0.543443  125.25.226.110  10.10.1.110     HTTP  HTTP/1.0 200 OK  (text/html)
20  0.543473  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=403 Ack=4196 Win=14528 Len=0
21  0.617404  125.25.226.110  10.10.1.110     HTTP  HTTP/1.0 200 OK  (text/css)
22  0.617435  10.10.1.110     125.25.226.110  TCP   49186 > 80 [ACK] Seq=413 Ack=1061 Win=8000 Len=0
24  3.636191  10.10.1.110     125.25.226.110  HTTP  GET /favicon.ico HTTP/1.1
25  3.636756  125.25.226.110  10.10.1.110     TCP   80 > 49185 [ACK] Seq=4196 Ack=893 Win=7936 Len=0
26  3.688722  125.25.226.110  10.10.1.110     HTTP  HTTP/1.0 304 Not Modified
27  3.688745  10.10.1.110     125.25.226.110  TCP   49185 > 80 [ACK] Seq=893 Ack=4585 Win=17472 Len=0
```

Details of selected packets:

```
Frame 6 (468 bytes on wire, 468 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89), Dst: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45)
Internet Protocol, Src: 10.10.1.110 (10.10.1.110), Dst: 125.25.226.110 (125.25.226.110)
Transmission Control Protocol, Src Port: 49185 (49185), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 402
Hypertext Transfer Protocol

Frame 8 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49185 (49185), Seq: 1, Ack: 403, Len: 1448

Frame 10 (143 bytes on wire, 143 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49185 (49185), Seq: 1449, Ack: 403, Len: 77

Frame 15 (478 bytes on wire, 478 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89), Dst: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45)
Internet Protocol, Src: 10.10.1.110 (10.10.1.110), Dst: 125.25.226.110 (125.25.226.110)
Transmission Control Protocol, Src Port: 49186 (49186), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 412
Hypertext Transfer Protocol

Frame 17 (1474 bytes on wire, 1474 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49185 (49185), Seq: 1526, Ack: 403, Len: 1408

Frame 19 (1328 bytes on wire, 1328 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49185 (49185), Seq: 2934, Ack: 403, Len: 1262
[Reassembled TCP Segments (4195 bytes): #8(1448), #10(77), #17(1408), #19(1262)]
Hypertext Transfer Protocol
Line-based text data: text/html
```

```
Frame 21 (1126 bytes on wire, 1126 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49186 (49186), Seq: 1, Ack: 413, Len: 1060
Hypertext Transfer Protocol
Line-based text data: text/css

Frame 24 (556 bytes on wire, 556 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89), Dst: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45)
Internet Protocol, Src: 10.10.1.110 (10.10.1.110), Dst: 125.25.226.110 (125.25.226.110)
Transmission Control Protocol, Src Port: 49185 (49185), Dst Port: 80 (80), Seq: 403, Ack: 4196, Len: 490
Hypertext Transfer Protocol

Frame 26 (455 bytes on wire, 455 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45 (00:50:ba:4c:6b:45), Dst: 00:17:31:5a:e5:89 (00:17:31:5a:e5:89)
Internet Protocol, Src: 125.25.226.110 (125.25.226.110), Dst: 10.10.1.110 (10.10.1.110)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49185 (49185), Seq: 4196, Ack: 893, Len: 389
Hypertext Transfer Protocol
```

Question 9 [7 marks]

The following shows the contents of the file for a computer. Answer the questions based only on this output.

```
lease {
  interface "eth0";
  fixed-address 10.10.1.42;
  option subnet-mask 255.255.255.0;
  option routers 10.10.1.2;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option domain-name-servers 10.10.6.34;
  option dhcp-server-identifier 10.10.1.6;
  option netbios-name-servers 192.168.1.6,10.10.1.5;
  renew 4 2008/11/6 16:12:00;
  rebind 5 2008/11/7 03:26:15;
  expire 5 2008/11/7 06:26:15;
}
```

a) What is the name of the file? [1 mark]

Answer

/var/lib/dhcp3/dhclient.leases

b) What protocol is this information used by? [1 mark]

Answer

DHCP – Dynamic Host Configuration Protocol

c) What is the purpose of the protocol? [1 mark]

Answer

For a client to automatically obtain an IP address from a server.

d) What is the IP address of the computer that has this file? [1 mark]

Answer

10.10.1.42

e) What is the IP address of the computer that provided the information stored in this file? [1 mark]

Answer

DHCP server: 10.10.1.6

f) Explain what the *renew* line means. [1 mark]

Answer

The time before which the computer should contact DHCP server 10.10.1.6 if it wants to continue using the lease.

g) Explain what the *rebind* line means. (The difference from renew should be clearly stated) [1 mark]

Answer

Assuming no response from 10.10.1.6, the time before which the computer should contact any DHCP server to request continue using the leased IP address.

Question 10 [8 marks]

The following shows the text output from a packet capture in Wireshark. The details of two packets/frames are shown (Frame 4 and Frame 8).

```
Frame 4 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: 00:23:69:3a:f4:7d, Dst: 00:17:31:5a:e5:89
    Destination: 00:17:31:5a:e5:89
    Source: 00:23:69:3a:f4:7d
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.1.184, Dst: 192.168.1.2
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
    Total Length: 88
    Identification: 0x7893 (30867)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x33e6 [correct]
    Source: 10.10.1.184 (10.10.1.184)
    Destination: 192.168.1.2 (192.168.1.2)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 1 (Host unreachable)
    Checksum: 0xc9f8 [correct]
    Data

Frame 8 (105 bytes on wire, 105 bytes captured)
Ethernet II, Src: 00:23:69:3a:f4:7d, Dst: 00:17:31:5a:e5:89
    Destination: 00:17:31:5a:e5:89
    Source: 00:23:69:3a:f4:7d
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.1.22 , Dst: 192.168.1.2
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 91
    Identification: 0xd880 (55424)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: TCP (0x06)
    Header checksum: 0x9652 [correct]
    Source: 10.10.1.22
    Destination: 192.168.1.2
Transmission Control Protocol, SrcPort: 22, DstPort: 60772, Seq:1, Ack:1, Len:39
    Source port: 22
    Destination port: 60772
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 40    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x18 (PSH, ACK)
    Window size: 5888 (scaled)
    Checksum: 0xac15 [correct]
    Options: (12 bytes)
SSH Protocol
    Protocol: SSH-2.0-OpenSSH_5.1p1 Debian-5ubuntu1\r\n
```

a) For each frame, what is the highest layer protocol in use? [2 marks]

   i. Frame 4: ______________________________

   ii. Frame 8: ______________________________

Answers

Frame 4: ICMP

Frame 8: SSH

b) For each frame, draw the packet structure indicating all layers down to at least layer 2. Also, for each header/data, indicate the length in bytes. [6 marks]

   i. Frame 4:

   ii. Frame 8:

Answer

Frame 4: Ethernet (14) | IP (20) | ICMP (68)

Frame 8: Ethernet (14) | IP (20) | TCP (32) | SSH (39)

Question 11 [4 marks]

The following shows the output of a tracepath command. Answer the questions based only on this output.

```
sgordon@ginger:~$ tracepath bridge.siit.tu.ac.th
 1:  ginger.local (10.10.1.171)                             0.122ms pmtu 1500
 1:  bkd-fac.siit.tu.ac.th (10.10.1.1)                      1.589ms
 2:  10.10.10.1 (10.10.10.1)                                1.955ms
 3:  192.168.72.3 (192.168.72.3)                          asymm  4   3.370ms
 4:  192.168.74.2 (192.168.74.2)                          asymm  5 735.108ms
 5:  192.168.73.1 (192.168.73.1)                          450.206ms
 6:  bridge.siit.tu.ac.th (192.168.10.1)                  847.116ms reached
```

a) How many routers between the source of the tracepath command and the destination given in the tracepath command? [1 mark]

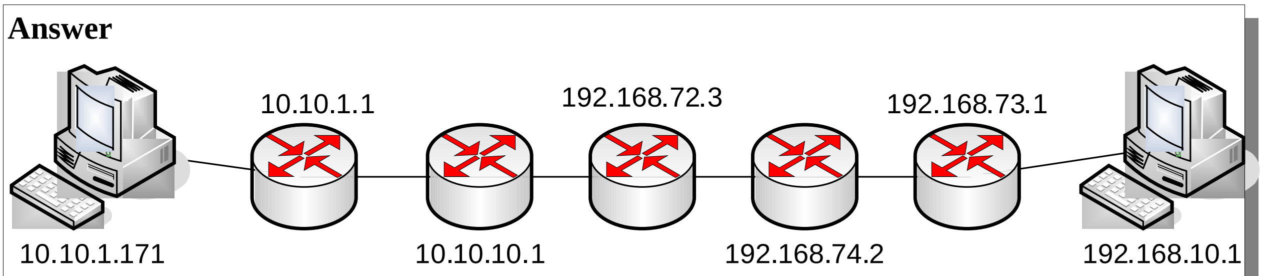
Answer

5

b) Draw a diagram that shows the connections between devices for the path shown. Each device must be labeled with:

- IP address of the device
- Source, Destination or Router (that is, give each device a label that indicates whether that device is a Source, Destination or Router in the path). [3 marks]

Answer


10.10.1.1
192.168.72.3
192.168.73.1
10.10.1.171
10.10.10.1
192.168.74.2
192.168.10.1