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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination Answers: Semester 2/2008

Course Title : ITS332 Information Technology II Laboratory

Instructor : Dr Steven Gordon

Date/Time : Friday 9 January 2009, 13:30 to 16:30

Instructions:

- This examination paper has 21 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.
- Assume 8 bits = 1 Byte; 1000 Bytes = 1KB; 1000KB = 1MB; 1000MB = 1GB; ...

Questions [84 marks]

Question 1 [14 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 program (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) Explain the `lo` interface and give an example of how it may be used. [1 mark]

Answer

The `lo` interface is the loopback interface. A computer that sends a packet to the loopback interface has the packet delivered to itself. This can be used for example for testing applications on the computer such as seeing if the application or protocol software can send packets or to see if a server is running on the computer.

e) What is the maximum size of a packet that can be sent on `eth1`? [1 mark]

Answer

1500 Bytes (since the Maximum Transmission Unit (MTU) is 1500).

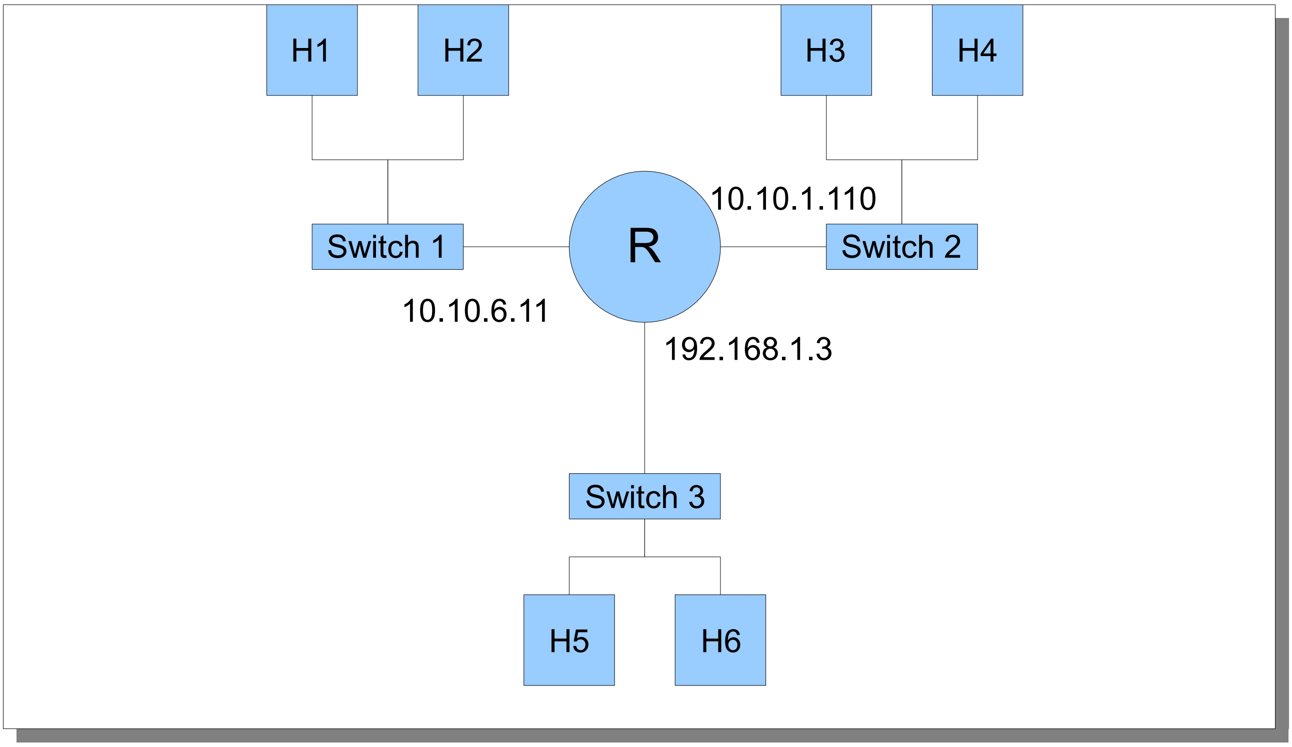
f) What is the average size of a packet received on `eth4`? [1 mark]

Answer

107 Bytes. Total bytes received is 33101632 while the number of packets received is 308380. Therefore the average size is 33101632/308380 = 107 Bytes.

g) Assume the computer *R* is a router, with two hosts connected, via a switch, to each interface of *R*. Draw a diagram that illustrates the network, showing the router, switches, hosts and the IP addresses of all interfaces. [4 marks]

Answer



h) In the network, which hosts receive the most traffic? Give their IP addresses and explain why [2 marks].

Answer

The hosts attached to interface `eth4`. If you look at the total traffic sent and received on each interface the majority (311MB) is sent by `eth4`. Therefore, the hosts attached to this network receive the most traffic.

i) In the network, do you think router *R* generates any data (that is, *R* is the source of data)? Give a yes or no answer and explain why. (Apart from devices listed in part (g), assume no other devices are in the network) [2 marks].

Answer

Yes. The total traffic received by the router (31 + 78 + 12 = 121MB) is less than the total traffic sent by the router (311 + 2 + 31 = 344MB). Therefore, the router must generate some traffic (223MB to `eth4`).

Question 2 [8 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 5 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=50 time=29.7 ms
64 bytes from 203.131.209.77: icmp_seq=2 ttl=50 time=27.3 ms
64 bytes from 203.131.209.77: icmp_seq=3 ttl=50 time=27.3 ms
64 bytes from 203.131.209.77: icmp_seq=4 ttl=50 time=29.6 ms
64 bytes from 203.131.209.77: icmp_seq=5 ttl=50 time=34.5 ms

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

_____ packets transmitted, _____ received, _____% packet loss, time 4008ms

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

a) Fill in the seven spaces in the ping statistics. For times, give your answer to the nearest 0.1 ms (for example, "2.4ms"). [0.5 marks for each answer].

Answer

The actual ping output is below.

```
sgordon@basil:~$ ping -c 5 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=50 time=29.7 ms
64 bytes from 203.131.209.77: icmp_seq=2 ttl=50 time=27.3 ms
64 bytes from 203.131.209.77: icmp_seq=3 ttl=50 time=27.3 ms
64 bytes from 203.131.209.77: icmp_seq=4 ttl=50 time=29.6 ms
64 bytes from 203.131.209.77: icmp_seq=5 ttl=50 time=34.5 ms

--- www.siit.tu.ac.th ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 27.324/29.712/34.514/2.624 ms
```

The answers can easily be calculated. The -c option in the command line indicates the number of packets to be transmitted (5). There are 5 packets received from 203.131.209.77, meaning 0% packet loss. The minimum (27.3), average (29.7), maximum (34.5) and deviation (2.4) of the 5 times can be calculation. (The answers do not have to be as accurate as the actual ping output, which in fact uses more accurate values than those reported for each packet).

b) How many routers do you think are between the computer *C* and `www.siit.tu.ac.th`? Explain your answer. [3 marks]

Answer

14 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 14 routers to be received with a value of 50. (Although it is not practical, you may assume other initial values, such as 255).

Below are the results of another ping command on computer *C* to the same destination (www.siit.tu.ac.th). The summary statistics are hidden.

```
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=50 time=34.4 ms
64 bytes from 203.131.209.77: icmp_seq=2 ttl=50 time=32.9 ms
64 bytes from 203.131.209.77: icmp_seq=3 ttl=50 time=29.1 ms
64 bytes from 203.131.209.77: icmp_seq=4 ttl=50 time=38.9 ms
64 bytes from 203.131.209.77: icmp_seq=5 ttl=50 time=37.8 ms

--- www.siit.tu.ac.th ping statistics ---
___ packets transmitted, ___ received, ___% packet loss, time 2004ms
rtt min/avg/max/mdev = ___/___/___/___ ms
```

The times reported are obviously different (e.g. 29.7ms versus 34.4ms).

c) When the user on computer *C* executed this second ping command, what did they do differently from the first ping? Explain your answer. [1.5 marks]

Answer

In both cases 5 ICMP requests where sent, however the total time is different (4s vs 2s). The interval between requests is reduced (using the -i option) in the second case to 0.5sec (compared to the default 1sec).

Question 3 [6 marks]

The following shows output from several commands on a computer *C*. Answer the questions based only on this output.

```
sgordon@ginger:~$ netstat -t -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.10.1.110:38331       63.150.131.190:80       ESTABLISHED
tcp        0      0 10.10.1.110:58685       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:58683       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:54299       125.25.226.110:22       ESTABLISHED
tcp        0      0 10.10.1.110:57025       10.10.6.11:22           ESTABLISHED
tcp        0      0 10.10.1.110:38333       63.150.131.190:80       ESTABLISHED
tcp        0      0 10.10.1.110:58682       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:39756       207.46.30.34:80         ESTABLISHED
tcp        0      0 10.10.1.110:58681       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:60955       209.85.143.83:80        ESTABLISHED
tcp        0      0 10.10.1.110:58680       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:58684       203.131.209.77:80       ESTABLISHED
tcp        0      0 10.10.1.110:38332       63.150.131.190:80       ESTABLISHED

sgordon@ginger:~$ nslookup www.siit.tu.ac.th
Server:         10.10.10.9
Address:  10.10.10.9#53

Name:    www.siit.tu.ac.th
Address: 203.131.209.77

sgordon@ginger:~$ nslookup mail.google.com
Server:         10.10.10.9
Address:  10.10.10.9#53

Non-authoritative answer:
mail.google.com    canonical name = googlemail.l.google.com.
Name:    googlemail.l.google.com
Address: 209.85.143.18
Name:    googlemail.l.google.com
Address: 209.85.143.19
Name:    googlemail.l.google.com
Address: 209.85.143.83
```

a) How many web sites do you think the user on computer *C* is visiting? Explain your answer. [1 mark]

Answer

4 or 11 are valid answers. 11 because there are 11 foreign addresses with port number 80 (identifying a web server). However, several of the foreign addresses are repeats, which suggests although the user is visiting one site, multiple TCP connections may be opened to that site by the browser.

b) In which of the following files would you find the abbreviated name of the server that computer *C* is connected to which isn't a web server? [Multiple choice, select only one answer, 1 mark]

i. `/etc/hosts`

ii. `/etc/services`

iii. `/etc/resolv.conf`

iv. `/var/www/index.html`

v. `/proc/sys/net/ipv4/ip_forward`

vi. `/etc/apache2/apache.conf`

Answer

`/etc/services`. This lists port numbers and corresponding server names. Port number 22 is ssh.

c) What port number does a DNS server use? [1 mark]

Answer

53. This can be seen from the output of `nslookup`, which displays the server and port number the computer contacted to find the IP address for the requested domain name.

d) What is computer *C*'s default DNS server? [1 mark]

Answer

10.10.10.9

e) What does the "Local Address" column of `netstat` output report? That is, explain *what* the two addresses identify. [2 marks]

Answer

The Local Address identifies the IP address of this computer (10.10.1.110) as well as the port number of the application on this computer (e.g. 38331).

Question 4 [18 marks]

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

a) What URL did the user first type into their browser? Explain how you know the answer. [2 marks]

Answer

www.sandilands.info/siit/index.html. The DNS query indicates a domain name was typed in (rather than IP address). The file requested in the HTTP GET request is /siit/index.html.

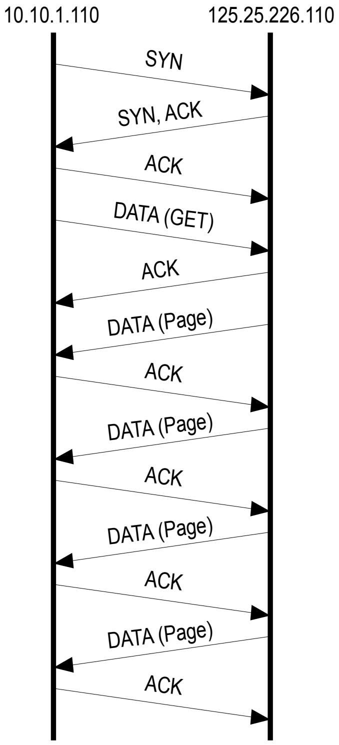
b) How many TCP connections are captured? Explain your answer. (Hint: DNS does not use TCP) [2 marks]

Answer

2. A TCP connection is identified by source IP, destination IP, source port, destination port. The IP addresses are 10.10.1.110 and 125.25.226.110, the destination port is 80, but the client uses two different source ports (49185 and 49186), hence 2 TCP connections.

c) 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) [6 marks]

Answer



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
```

b) The MAC address 00:17:31:5a:e5:89 belongs to which device (or computer) in the network? (Give a description or name of the device, not the IP address). [1 mark]

Answer

The source computer requesting the web page.

c) The MAC address 00:50:ba:4c:6b:45 belongs to which device (or computer) in the network? (Give a description or name of the device, not the IP address). [1 mark]

Answer

The next (or default) router from the source computer.

d) List all URLs that have been requested using a HTTP GET request. [1.5 marks]

Answer

www.sandilands.info/siit/index.html

www.sandilands.info/siit/css/site.css

www.sandilands.info/favicon.ico

e) For each of the above requests sent by the source computer, explain the HTTP response received by the source computer (e.g. what type of response was received? why? What data (if any) is in the response?). [3 marks]

Answer

www.sandilands.info/siit/index.html: HTTP 200 Ok is received. This means the page is returned in the response (it was available on the server).

www.sandilands.info/siit/css/site.css: HTTP 200 Ok received. Same as above.

www.sandilands.info/favicon.ico: HTTP 304 Not Modified received. This means the page requested has not been modified since the last request. The page is not included in the response.

f) For each HTTP response indicate the size of the HTTP response (including any data). [1.5 marks]

Answer

www.sandilands.info/siit/index.html: 4195 Bytes (frame 19)

www.sandilands.info/siit/css/site.css: 1060 Bytes (frame 21)

www.sandilands.info/favicon.ico: 389 Bytes (frame 26)

Question 5 [10 marks]

The following shows the contents of the file `/var/lib/dhcp3/dhclient.leases` for a computer. Answer the questions based only on this output.

```
lease {
  interface "eth0";
  fixed-address 10.10.1.110;
  option subnet-mask 255.255.255.0;
  option routers 10.10.1.1;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option domain-name-servers 10.10.6.34;
  option dhcp-server-identifier 10.10.1.1;
  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 protocol is this information used by? [1 mark]

Answer

DHCP – Dynamic Host Configuration Protocol

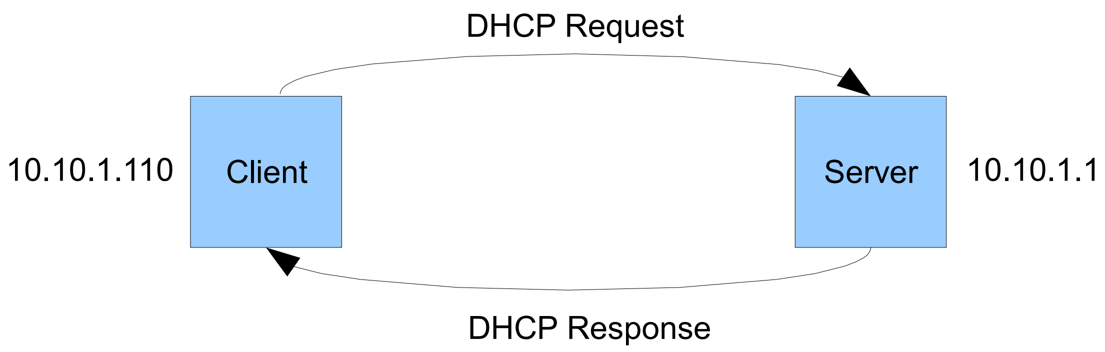
b) What is the purpose of the protocol? [1 mark]

Answer

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

c) Draw a diagram of a network that shows the devices involved in this protocol, and illustrate how the protocol works by drawing/labelling the messages on the diagram. For each device involved in the protocol, give its IP address. [5 marks]

Answer



d) What is the maximum time that the computer can use its IP address before contacting the server again? [1 mark]

Answer

86400 seconds

e) During normal operation, at what time will the computer contact the server to continue using the IP address? Explain your answer. [1 mark]

Answer

The computer will renew its IP address on (or before) 6/11/2008 at 16:12:00.

f) What is the IP address of the server that the computer will contact to map `www.google.com` to an IP address? Explain your answer. [1 mark]

Answer

To map domain name to IP address a Domain Name Server will be used: 10.10.6.34.

Question 6 [6 marks]

The following shows the text output from a packet capture in Wireshark. The details of two frames captured are shown. Answer the questions based only on this output.

```
Frame 1 (42 bytes on wire, 42 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
        Address: ff:ff:ff:ff:ff:ff
        IG bit: Group address (multicast/broadcast)
        LG bit: Locally administered address (this is NOT the factory default)
    Source: 00:17:31:5a:e5:89
        Address: 00:17:31:5a:e5:89
        IG bit: Individual address (unicast)
        LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:17:31:5a:e5:89
    Sender IP address: 10.10.1.110
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.10.1.33

Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:13:49:2b:7f:0b, Dst: 00:17:31:5a:e5:89
    Destination: 00:17:31:5a:e5:89
        Address: 00:17:31:5a:e5:89
        IG bit: Individual address (unicast)
        LG bit: Globally unique address (factory default)
    Source: 00:13:49:2b:7f:0b
        Address: 00:13:49:2b:7f:0b
        IG bit: Individual address (unicast)
        LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 00:13:49:2b:7f:0b
    Sender IP address: 10.10.1.33
    Target MAC address: 00:17:31:5a:e5:89
    Target IP address: 10.10.1.110
```

a) What protocol was in use that triggered the sending of these two frames? [1 mark]

Answer

ARP – Address Resolution Protocol

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

Answer

ARP is used for a host to determine the MAC address of a device with a given IP address.

c) Draw both packets, indicating all layers down to at least layer 2. [2 marks]

Answer

Frame 1: Ethernet | ARP

Frame 2: Ethernet | ARP

d) For each frame, explain which node sent the frame, what the frame means (i.e. the purpose of the frame) and where they sent the frame to (i.e. destination)? Use an appropriate address to refer to nodes. [2 marks]

Answer

Frame 1: sent by 10.10.1.110 to the broadcast address (everyone), in search of the comptuer with IP address 10.10.1.33

Frame 2: sent by 10.10.1.33 to 10.10.1.110 informing it of 10.10.1.33's MAC address

Question 7 [8 marks]

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

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.1.0       0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.3.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.3.0     10.10.3.4       255.255.255.0   UG    0      0        0 eth1
72.16.0.0       10.10.3.4       255.255.0.0     UG    0      0        0 eth1
10.10.2.0       10.10.1.1       255.255.255.0   UG    0      0        0 eth0
0.0.0.0         10.10.1.1       0.0.0.0         UG    0      0        0 eth0
```

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

Answer

```
route
```

b) How many LAN cards does this computer have? Explain your answer. [1 mark]

Answer

2 (at least). Since the interfaces listed in the routing table are eth0 and eth1 (which identify Ethernet interfaces).

c) If computer *C* has an IP packet with one of the following destination addresses, then explain what is the next device that *C* sends the packet to, and what interface *C* uses to send the packet. Refer to devices using their IP address. In your explanation, refer to the row in the table that matches (e.g. rows 1 through to 6).

i. 10.10.1.110 [1 mark]

Answer

Row 1 matches. Send directly to 10.10.1.110 via interface eth0.

ii. 192.168.4.1 [1 mark]

Answer

Row 6 matches. Send to gateway 10.10.1.1 via interface eth0.

iii. 72.16.0.10 [1 mark]

Answer

Row 4 matches. Send to gateway 10.10.3.4 via interface eth1.

iv. 10.10.2.1 [1 mark]

Answer

Row 5 matches. Send to gateway 10.10.1.1 via interface eth0.

d) If the following command was executed on computer *C*, would any of your answers to part (c) change? Explain your answer. [2 marks]

```
route del -net 10.10.2.0 netmask 255.255.255.0 gw 10.10.1.1 eth0
```

Answer

Yes. A route is deleted (the 5th row). However the packet destined to 10.10.2.1 would still be sent to 10.10.1.1 via interface eth0 because that is the default gateway.

Question 8 [6 marks]

Assume you want to configure a peer-to-peer network between two computers at home. Assume computer A has an IP address of 192.168.1.34 and subnet mask 255.255.255.0.

a) For computer B, indicate if the following addresses are needed, and what they should be set to:

i. IP address [1 mark]

Answer

Any address in the range 192.168.1.1 to 192.168.1.254 except 192.168.1.34.

ii. Subnet mask [1 mark]

Answer

255.255.255.0

iii. Default gateway [1 mark]

Answer

Not needed.

b) What type of cable would you use to connect the two computers? [1 mark]

Answer

Cross-over cable

c) Which of the following commands (select zero or more) would you use to *configure* the computers so that the network worked? [1 mark]

`ping`, `ifconfig`, `route`, `arp`, `tracepath`, `dhclient`, `wireshark`, `hosts`, `nslookup`

Answer

`ifconfig`.

d) Which of the above set of commands (select zero or more) could you use to *test* that the network works by sending packets? [1 mark]

Answer

`ping` and `tracepath`.

Question 9 [8 marks]

a) Draw the network topology if the SIIT ICT Networking Lab and its connections to other networks (up until `bridge.siit.tu.ac.th`) assuming the following [7 marks]:

- ○ The lab has 2 PCs per group (instead of 9), and 2 groups (instead of 4).
- ○ The cabinets in the Lab have Ethernet connections to a switch in the Computer Centre; the switch also connects to a Router in the Computer Centre via Ethernet.
- ○ Use the output from `tracepath` (performed from a computer within the Lab) to determine the devices/connectivity up until `bridge.siit.tu.ac.th`. You do not need to draw any networks beyond `bridge.siit.tu.ac.th`.
- ○ You should label each device as either a host, switch or router. Give IP addresses of the devices when they are available.

```
$ tracepath bridge.siit.tu.ac.th
 1:  10.10.6.11 (10.10.6.11)                                  0.127ms pmtu 1500
 1:  10.10.6.1 (10.10.6.1)                                    0.794ms
 2:  10.10.10.1 (10.10.10.1)                                  1.919ms
 3:  192.168.72.3 (192.168.72.3)                            asymm  4   2.921ms
 4:  192.168.79.2 (192.168.79.2)                            asymm  5 209.821ms
 5:  192.168.73.1 (192.168.73.1)                            276.766ms
 6:  bridge.siit.tu.ac.th (192.168.10.1)                    276.816ms reached
     Resume: pmtu 1500 hops 6 back 6
```

Answer

b) How many IP subnets are shown in your diagram? [1 mark]

Answer

6.