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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2007

Course Title : ITS 332 – Information Technology II Lab (Networking)

Instructor : Dr Steven Gordon

Date/Time : Wednesday 9 January 2008, 13:30 – 16:30

Instructions:

- This examination paper has 15 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, **Non-programmable calculator 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.

General Questions [60 marks]

Question 1 [6 marks]

The following shows interface configuration information for a computer. Answer the questions based only on this output.

```
eth0      Link encap:Ethernet  HWaddr 00:17:31:5A:E5:89
          inet addr:10.10.1.171  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:220 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:40000 (39.1 KiB)  TX bytes:10000 (9.8 KiB)
          Base address:0xd800 Memory:cffe0000-d0000000

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:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 b)  TX bytes:100 (100.0 b)
```

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

ifconfig

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

1

c) Explain what the `lo` interface is used for. [1 mark]

Loopback. For a computer to send a packet to itself. Used for testing.

d) What is the IP address of the Ethernet card? [1 mark]

10.10.1.171

e) What is the MAC (Physical) address of the Ethernet card? [1 mark]

00:17:31:5A:E5:89

f) What is the average size of packets transmitted by the Ethernet card? [1 mark]

200 bytes

Question 2 [5 marks]

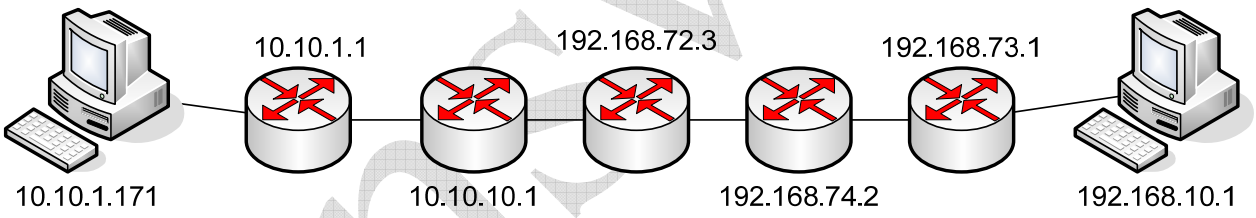
The following shows the output of a `tracepath` command. Answer the questions based only on this output.

```
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]

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). [4 marks]

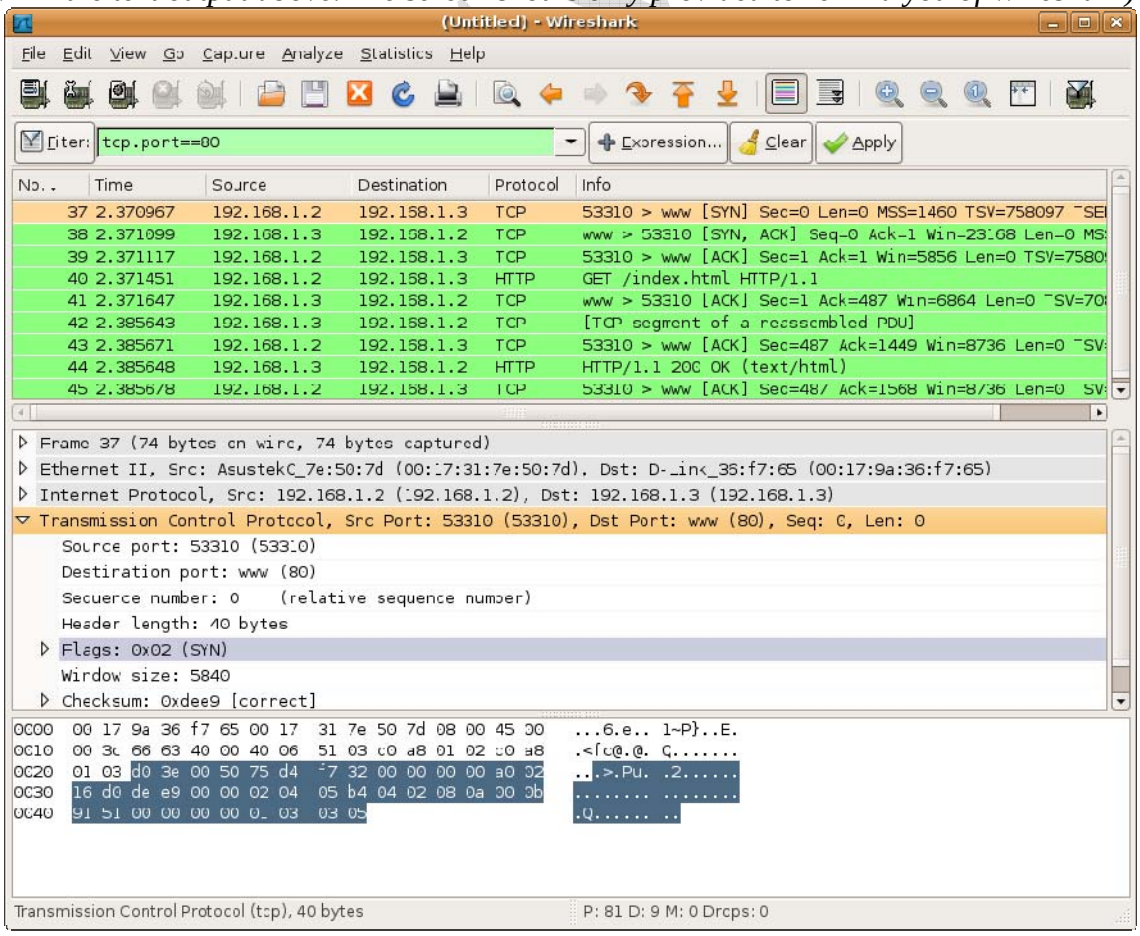


Question 3 [11 marks]

The following shows the text output from a packet capture in Wireshark. The text output is identical to the information seen in Wireshark (for example, the text output showing 9 captured packets is identical to the information in the top part of the screen in the following figure). The text output is given because it is easier to read than the screen capture. Use the text output to answer the questions. (Note that all packets captured are not shown, that is, a display filter has been applied). Answer the questions based only on the text output in this question.

```
No.  Time       Source        Destination   Prot  Info
37   2.370967   192.168.1.2   192.168.1.3   TCP   53310 > www [SYN] Seq=0 Len=0
                                                   MSS=1460
38   2.371099   192.168.1.3   192.168.1.2   TCP   www > 53310 [SYN, ACK] Seq=0
                                                   Ack=1 Win=23168 Len=0 MSS=1460
39   2.371117   192.168.1.2   192.168.1.3   TCP   53310 > www [ACK] Seq=1 Ack=1
                                                   Win=5856 Len=0
40   2.371451   192.168.1.2   192.168.1.3   HTTP  GET /index.html HTTP/1.1
41   2.371647   192.168.1.3   192.168.1.2   TCP   www > 53310 [ACK] Seq=1 Ack=487
                                                   Win=6864 Len=0
42   2.385643   192.168.1.3   192.168.1.2   TCP   [segment of a reassembled PDU]
43   2.385671   192.168.1.2   192.168.1.3   TCP   53310 > www [ACK] Seq=487
                                                   Ack=1449 Win=8736 Len=0
44   2.385648   192.168.1.3   192.168.1.2   HTTP  HTTP/1.1 200 OK (text/html)
45   2.385678   192.168.1.2   192.168.1.3   TCP   53310 > www [ACK] Seq=487
                                                   Ack=1568 Win=8736 Len=0
```

(You do not need to use the following screen shot of Wireshark – the necessary information is shown in the text output above. The screen shot is only provided to remind you of Wireshark)



a) Draw a diagram that illustrates the exchange of packets shown in the capture. Make sure you clearly label the IP addresses of the nodes, as well as the message types. [4 marks]

b) What is the application protocol used in this capture? [1 mark]

HTTP or Hypertext Transfer Protocol

c) Which packets are part of the TCP connection setup? (Give the packet numbers – you can select from packet 37 through to 45) [1 mark]

37, 38 and 39

d) What port number is the client application using? [1 mark]

55310

The following output shows the detail of a single frame: Frame 40. The output is identical to what you would see if you expanded all fields in the middle section of the Wireshark window. Answer the following questions based on this output, as well as the packet list output on the previous page.

```
Frame 40 (552 bytes on wire, 552 bytes captured)
    Arrival Time: Jan  5, 2008 14:17:07.761857000
    [Time delta from previous captured frame: 0.000334000 seconds]
    [Time delta from previous displayed frame: 0.000334000 seconds]
    [Time since reference or first frame: 2.371451000 seconds]
    Frame Number: 40
    Frame Length: 552 bytes
    Capture Length: 552 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
```

```
Ethernet II, Src: 00:17:31:7e:50:7d, Dst: 00:17:9a:36:f7:65
    Destination: D-Link_36:f7:65 (00:17:9a:36:f7:65)
        Address: D-Link_36:f7:65 (00:17:9a:36:f7:65)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
    Source: AsustekC_7e:50:7d (00:17:31:7e:50:7d)
        Address: AsustekC_7e:50:7d (00:17:31:7e:50:7d)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.2, Dst: 192.168.1.3
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 538
    Identification: 0x6665 (26213)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x4f23 [correct]
        [Good: True]
        [Bad : False]
    Source: 192.168.1.2 (192.168.1.2)
    Destination: 192.168.1.3 (192.168.1.3)
Transmission Control Protocol, Src Port: 53310, Dst Port: www (80), Seq: 1,
Ack: 1, Len: 486
    Source port: 53310 (53310)
    Destination port: www (80)
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 487    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x18 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 5856 (scaled)
    Checksum: 0x6a70 [correct]
        [Good Checksum: True]
        [Bad Checksum: False]
    Options: (12 bytes)
        NOP
        NOP
        Timestamps: TSval 758097, TSecr 7089731
Hypertext Transfer Protocol
    GET /index.html HTTP/1.1\r\n
        Request Method: GET
        Request URI: /index.html
        Request Version: HTTP/1.1
```

```
    Host: 192.168.1.3\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.11)
                Gecko/20071127 Firefox/2.0.0.11\r\n
    Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.
8,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie:
SESS1a68f8b7bde2e267c86b0d605b3435be=0f97fc800b25326a600d1833ecf44989\r\n
    \r\n
```

e) Explain the most likely action of the user on the client computer to generate the packets captured (that is, what did the user do?). [1 mark]

In a web browser the user entered the address http://192.168.1.3/index.html (or clicked on a link to that address)

f) What operating system was the client user using (and explain why)? [1 mark]

Linux. The User-Agent header in the GET request indicates the OS.

g) Draw the packet for Frame 40, clearly showing the packet headers and their sizes. [3 marks]

Question 4 [4 marks]

The following shows the text output from a packet capture in Wireshark. The summary information for each packet is shown (note that all packets captured are not shown, that is, a display filter has been applied). Answer the questions based only on this output.

```
No.     Time        Source        Destination    Protocol Info
      4 1.681604    10.10.1.171   10.10.1.1      ICMP     Echo (ping) request
      5 1.681842    10.10.1.1     10.10.1.171    ICMP     Echo (ping) reply
      8 4.684437    10.10.1.171   10.10.1.1      ICMP     Echo (ping) request
      9 4.684828    10.10.1.1     10.10.1.171    ICMP     Echo (ping) reply
     13 7.684638    10.10.1.171   10.10.1.1      ICMP     Echo (ping) request
     14 7.684819    10.10.1.1     10.10.1.171    ICMP     Echo (ping) reply
```

a) Multiple Choice: Which command was most likely used to generate the traffic captured? [1 mark]

```
i.      ping –s 1000 –c 1 10.10.1.1
ii.     ping –s 1000 10.10.1.171
iii.    ping 10.10.1.1
iv.     ping –i 3 10.10.1.1
v.      ping –i 2 –c 3 10.10.1.1
```

iv.

b) Draw a diagram that shows the exchange of packets that have been captured. [3 marks]

Question 5 [7 marks]

The following shows the contents of the file `/var/lib/dhcp3/dhclient.eth0.leases` for a computer. Answer the questions based only on this output.

```
lease {
  interface "eth0";
  fixed-address 10.10.1.73;
  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 10.10.10.9,192.168.20.103;
  option dhcp-server-identifier 10.10.10.2;
  option netbios-name-servers 10.10.1.5,192.168.1.6,192.168.2.2;
  renew 5 2008/1/4 15:21:39;
  rebind 6 2008/1/5 03:03:04;
  expire 6 2008/1/5 06:03:04;
}
```

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

DHCP or Dynamic Host Configuration Protocol

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

Automatically assigned IP addresses to computers

c) What IP address has been assigned to the computer? [1 mark]

10.10.1.73

d) What is the IP address of the server that assigned an IP address to this computer? [1 mark]

10.10.10.2

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

86400 seconds

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

15:21:39 on 2008/1/4

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

10.10.10.9 or 192.168.20.103

Question 6 [5 marks]

For the following questions, give short (one word or sentence) answers.

a) What will the command `arp` display? [1 mark]

Displays the mapping of IP addresses to hardware addresses that the computer knows of.

b) What is the purpose of the commands `ifup` and `ifdown`? [1 mark]

To turn a particular network interface card up (start, on) or down (stop, off)

c) What type of Ethernet cable should you use to connect a computer (host) to a router? [1 mark]

Cross-over cable

d) What type of Ethernet cable should you use to connect a router to a switch? [1 mark]

Straight-through cable

e) When configuring two computers in a peer-to-peer network, is a gateway needed? Explain why or why not. [1 mark]

No. A gateway connects one network to another. If there is only 1 network, then no need for a gateway.

Question 7 [7 marks]

The following shows the text output from a packet capture in Wireshark. The summary information for each packet is shown (note that all packets captured are not shown, that is, a display filter has been applied). In addition, detailed information for each packet (frame) is shown (similar to what you would see in the middle section of Wireshark). Answer the questions based only on the output in this question.

```
No. Time        Source        Destination  Protocol Info
5   10.046891   10.10.1.171   10.10.10.9   DNS      Standard query A
6   10.048204   10.10.10.9    10.10.1.171  DNS      Standard query response

Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89, Dst: 00:50:ba:be:34:df
Internet Protocol, Src: 10.10.1.171, Dst: 10.10.10.9
User Datagram Protocol, Src Port: 32779 (32779), Dst Port: domain (53)
Domain Name System (query)

Frame 6 (350 bytes on wire, 350 bytes captured)
Ethernet II, Src: 00:50:ba:be:34:df, Dst: 00:17:31:5a:e5:89
Internet Protocol, Src: 10.10.10.9, Dst: 10.10.1.171
User Datagram Protocol, Src Port: domain (53), Dst Port: 32779 (32779)
Domain Name System (response)
```

a) What application protocol is being used in the packet capture? [1 mark]

DNS or Domain Name System

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

To map domain names to IP addresses

c) How many milliseconds does it take for the source to obtain a response? [1 mark]

1413 ms

d) Draw the format of Frame 5, giving the names of headers and data. [1 mark]

e) Assuming a subnet mask of 255.255.255.0, is the destination of Frame 5 on the same network as the source of Frame 5? [1 mark]

No

f) What device in the network does the address `00:50:ba:be:34:df` correspond to? [1 mark]

Router

g) At what port number does the server receive queries? [1 mark]

53

Question 8 [8 marks]

Draw a diagram illustrating a switched Ethernet network with 4 computers (hosts), 1 switch and a router. The router is connected to another external network which has the network address 73.16.12.0 (you do not have to draw this external network – simply indicate it by a cloud or circle). For each relevant interface, indicate the IP address that you would configure it with. Assume a subnet mask of 255.255.255.0 for all computers (including external network). On the diagram indicate the types of Ethernet cables used.

Question 9 [3 marks]

The following shows the contents of the `/etc/network/interfaces` file on a computer. There is an error in the parameter values given. What is the error and what would you change to fix the error?

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.7
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway  192.168.12.1
```

The gateway address is that of a computer on another network. A computer's gateway should be on the same network as the computer. To fix, the gateway must be put on the same physical network, and therefore have a IP address on that network, e.g. 192.168.1.1.

Question 10 [4 marks]

The following shows the output of the `route` command. Answer the questions based only on this output.

```
Destination     Gateway    Genmask         Flags Metric Ref    Use  Iface
10.10.1.0       *          255.255.255.0   U     0      0        0  eth0
default         10.10.1.1  0.0.0.0         UG    0      0        0  eth0
```

If a computer has a packet with the following destination addresses, where will the packet be sent? Explain your answer, by referring to the output above (e.g. which entries in the table match and why).

a) 10.10.1.72

Will be sent directly to the destination since the first entry matches (10.10.1.72 is on network 10.10.1.0) and * for Gateway means send directly.

b) 10.10.10.1

Will be sent to the gateway 10.10.1.1, since the first entry does NOT match, and therefore the default (second) entry matches.

c) 10.10.1.1

Will be sent directly to the destination since the first entry matches (10.10.1.1 is on network 10.10.1.0) and * for Gateway means send directly.

d) 73.16.4.3

Will be sent to the gateway 10.10.1.1, since the first entry does NOT match, and therefore the default (second) entry matches.