Internet Protocols Final Exam

Name _____ Student ID _____

1. What is the purpose of the gratuitous ARP packets in the following trace? [5pts]

Duplicate address detection (DAD)

2 0.990599	192.168.1.1	192.168.1.100	DHCP	DHCP Offer	- Transaction ID 0x9053c394
3 0.994631	192.168.1.1	192.168.1.100	DHCP	DHCP ACK	- Transaction ID 0x9053c394
4 0.997848	AsustekC_75:81:4f	Broadcast	ARP	Gratuitous ARP for 192.168.1.100 (Request)	
5 1.985062	AsustekC_75:81:4f	Broadcast	ARP	Gratuitous ARP for 192.168.1.100 (Request)	
6 2.985102	AsustekC_75:81:4f	Broadcast	ARP	Gratuitous ARP for 192.168.1.100 (Request)	

2. When would my PC first try to renew the lease according to the `ipconfig` output? [5pts]

```
Connection-specific DNS Suffix  . : kornet
Description . . . . . . . . . . . : Realtek RTL8168/8111 PCI-E Gigabit Eth
Physical Address. . . . . . . . . : 00-1B-FC-75-**-**
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 218.153.157.237
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 218.153.157.1
DHCP Server . . . . . . . . . . . : 121.138.7.42
DNS Servers . . . . . . . . . . . : 168.126.63.1
                                   168.126.63.2
Lease Obtained. . . . . . . . . . : 2008년 6월 16일 월요일 오전 9:54:15
Lease Expires . . . . . . . . . . : 2008년 6월 16일 월요일 오전 10:54:15
```

Translation ☞ 월=Month, 일=Date, 월요일=Monday, 오전=A.M.

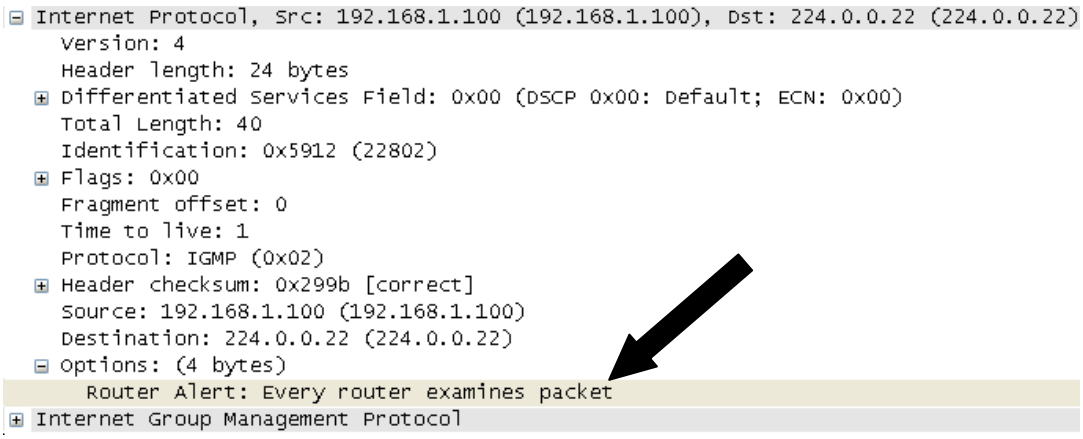
2008년 6월 16일 오전 10:24:15 (10:24:15 A.M. on 6/16/2008)

3. In Problem 2, where is the BOOTP Relay located? [5pts]

218.153.157.1

4. Although most IP options are useless today, IGMP v2 uses so called the Router Alert (RA) option as shown in the packet capture. With this option, the IP (multicast) router must look for the IGMP packet in the datagram. Why would you think the option is convenient? (Hint: consider the difference between simply forwarding an IP datagram destined to a multicast address and processing IGMP packet?) [10pts]

It can be used to force the router to process the IGMP message in the payload of an IP datagram; for multicast data packets the option does not have to be used since the router can forward them by just looking at the IP header.



5. In the following Wireshark capture, where do you think that the Nagle's Algorithm is achieving its intended purpose? Identify the data packet numbers [5pts] and explain why you think so [5pts].

Packets #48, #54 --- these are carrying more than 1 byte

```
39 2.448451 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=18 Win=5888 Len=0
40 2.459102 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
41 2.461724 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=19 Win=5888 Len=0
42 2.523101 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
43 2.526030 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=20 Win=5888 Len=0
44 2.526051 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
45 2.528330 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=21 Win=5888 Len=0
46 2.587259 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
47 2.589946 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=22 Win=5888 Len=0
48 2.589967 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
49 2.592815 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=24 Win=5888 Len=0
50 2.667038 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
51 2.669776 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=25 Win=5888 Len=0
52 2.763200 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
53 2.765907 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=26 Win=5888 Len=0
54 2.765929 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
55 2.768669 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=29 Win=5888 Len=0
56 2.811138 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
57 2.813768 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=30 Win=5888 Len=0
58 2.843069 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
59 2.845819 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=31 Win=5888 Len=0
60 2.845840 192.168.1.103 163.152.6.65  TCP  [TCP segment of a reassembled PDU]
61 2.848519 163.152.6.65  192.168.1.103 TCP  25 > 3037 [ACK] Seq=54 Ack=32 Win=5888 Len=0
```

6. What is the base-64 encoding of 01010000 10111111 00100011 ? [5pts]

00010100 00001011 00111100 00100011

7. What are the three pieces of information that must be "synchronized" upon TCP connection setup? [6pts]

Initial sequence number (ISN)

Maximum segment size (MSS)

Window size (or the availability at the receive socket buffer)

8. Suppose you are a mail server named bluehouse.go.kr. After connecting to mailhub-wh3.whitehouse.gov at TCP port 25, you want to deliver an email from mb@bluehouse.go.kr to obama@whitehouse.gov. Write down the SMTP commands and data in correct sequence to achieve the delivery of the email message, "I love soccer." [10pts]

HELO *bluehouse.go.kr*

MAIL FROM: mb@bluehouse.go.kr

RCPT TO: obama@whitehouse.gov

DATA

I love soccer.

.

QUIT

10. Most SNMP messages carry name-value pairs. What is the SMI type of the name? [5pts]

OBJECT IDENTIFIER

11. Suppose your side of TCP sent a SYN segment with a Window Scale option. Now you look for the Window Scale option in the arriving SYN/ACK segment from the peer TCP. How is the TCP Window Scale option being set to 0 (e.g. as in Problem 5) different from the option not being used? [10pts]

Window Scale 0 means that the TCP peer understands the other's WS option, but that it won't scale its own window advertisement; no Window Scale option means the option shall not be used for the connection at all.

12. I got the following responses from a mail server at Gmail (Google mail). See that the server recognizes VRFY command, but it effectively declines to confirm if the account (i.e., hyogon) exists. What do you think is the reason? [10pts]

Not allowing spammers to confirm and collect valid email addresses from this mail server.

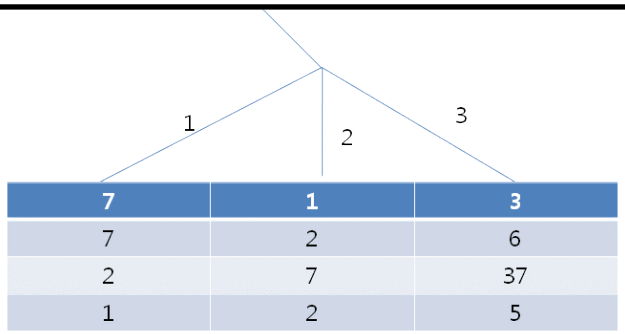
```
220 mx.google.com ESMTP k1si6320910ybe.115
EHLO babo.net
250-mx.google.com at your service, [218.153.157.211]
250-SIZE 35651584
250-8BITMIME
250 ENHANCEDSTATUSCODES
VRFY hyogon@gmail.com
252 2.1.5 Send some mail, I'll try my best k1si6320910ybe.115
```

13. Suppose a network management system (NMS) wants to read the following table at a managed device, and the OID of a row in the table is X, and columns 1 and 2 are used as the index.
    A. In order to get the value at position [3,3] (i.e., "37"), what OID instance should the NMS specify? [5pts]

X.3.2.7

    B. If the NMS issues the `getnext` of [2,2], what value does it get? [5pts]

5 (In lexicographic order, the 'next' of X.2.7.2 is X.3.1.2, whose value is 5)



14. Although not shown in the following packet sequence, there should be a query to DNS before the first packet (#17). What query type would it have? [4pts]

MX

```
17 1.132836 192.168.1.103 163.152.6.65   TCP  2641 > 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
18 1.137588 163.152.6.65  192.168.1.103  TCP  25 > 2641 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=7
19 1.137623 192.168.1.103 163.152.6.65   TCP  2641 > 25 [ACK] Seq=1 Ack=1 Win=256000 Len=0
20 1.141303 163.152.6.65  192.168.1.103  SMTP Response: 220 smtp.korea.ac.kr ESMTP Sat Jun 13 15:08:27 2009
21 1.230520 192.168.1.103 163.152.6.65   SMTP Command: EHLO P5B0720
22 1.234218 163.152.6.65  192.168.1.103  TCP  25 > 2641 [ACK] Seq=54 Ack=15 Win=5888 Len=0
23 1.234239 163.152.6.65  192.168.1.103  SMTP Response: 250-smtp.korea.ac.kr Hello [218.153.157.211]
24 1.392735 192.168.1.103 163.152.6.65   TCP  2641 > 25 [ACK] Seq=15 Ack=100 Win=255900 Len=0
25 1.395489 163.152.6.65  192.168.1.103  SMTP Response: 250-OUTBOUND_AUTH=Y
26 1.409645 192.168.1.103 163.152.6.65   SMTP Command: AUTH LOGIN
27 1.703550 163.152.6.65  192.168.1.103  SMTP [TCP Retransmission] Response: 250-OUTBOUND_AUTH=Y
28 1.703574 192.168.1.103 163.152.6.65   TCP  [TCP Dup ACK 26#1] 2641 > 25 [ACK] Seq=27 Ack=196 Win=255804 Len=0
29 3.806987 192.168.1.103 163.152.6.65   SMTP [TCP Retransmission] Command: AUTH LOGIN
30 3.849738 163.152.6.65  192.168.1.103  TCP  25 > 2641 [ACK] Seq=196 Ack=27 Win=5888 Len=0
31 3.852436 163.152.6.65  192.168.1.103  SMTP Response: 334 VXNlcm5hbWU6
32 3.852834 192.168.1.103 163.152.6.65   SMTP Command: aHlvz29u
33 3.855633 163.152.6.65  192.168.1.103  TCP  25 > 2641 [ACK] Seq=214 Ack=37 Win=5888 Len=0
34 3.855644 163.152.6.65  192.168.1.103  SMTP Response: 334 UGFzc3dvcmQ6
35 3.855786 192.168.1.103 163.152.6.65   SMTP Command: [redacted]
36 3.862309 163.152.6.65  192.168.1.103  SMTP Response: 235 Authentication success. SmtpAuth::AuthLogin() is_white=0
37 3.863077 192.168.1.103 163.152.6.65   SMTP Command: MAIL FROM: <hyogon@korea.ac.kr>
```

15. In UDP, a datagram destined to a port number for which there is no running process triggers the transmission of an ICMP destination (port) unreachable error. What happens if a TCP segment is sent to a port number that does not have a running process? [5pts]

TCP Reset segment is sent in response.