Internet Protocols Final Exam (2018. 6. 18)

<1 Hour>

*** You can answer in English or in Korean. 영어 또는 한국어로 답하시오. ***

Student ID **Name**

_____ _____답안지_____

1. Answer the following questions on DNS. **[5pts]**

   A. What is the self-imposed message size limit in the DNS protocol? 512 bytes

   B. How is it related with the minimum IP packet size processing capability of an IP interface? Briefly explain.
   Internet computers must be able to process minimum IP datagram size of 576 bytes. 512 is approximately the minimum IP size minus IP & UDP headers.

   C. Explain the other two things that happen when a DNS message is longer than the size limit above.

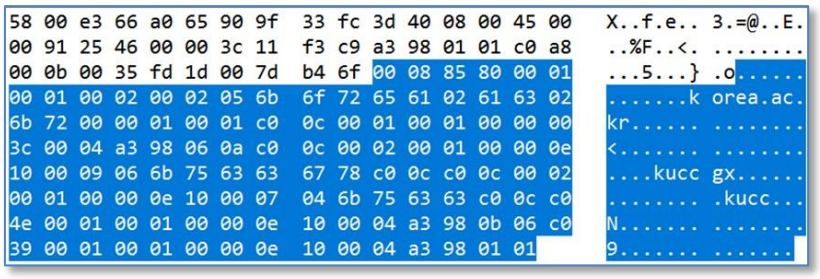
      i. DNS server: set the TC (truncated) flag to 1

      ii. DNS resolver (*i.e.*, client): discards the response.

      iii. DNS resolver: Question the same domain name using TCP this time

   D. Why does DNS use "compressed labels" in its packets? Because of the tight DNS message size limit in (A&B)

2. In the following packet trace, the shaded part is the DNS packet. Find the last compressed label in the packet, and write down the exact domain name that corresponds to the label. **[3pts]** **kucc.korea.ac.kr**



3. Given the following output from the `nslookup`, answer the following questions. **[19pts: 1pt** each except (L) and (M)]

```
> set querytype=MX
> korea.ac.kr
서버:    kuccgx.korea.ac.kr
Address:  163.152.1.1

korea.ac.kr     MX preference = 0, mail exchanger = spam.korea.ac.kr
korea.ac.kr     nameserver = kuccgx.korea.ac.kr
korea.ac.kr     nameserver = kucc.korea.ac.kr
spam.korea.ac.kr        internet address = 163.152.6.22
kucc.korea.ac.kr        internet address = 163.152.11.6
kuccgx.korea.ac.kr      internet address = 163.152.1.1
>
```

Donald sends an email to his friend Kim. Kim's email address is `kimj@korea.ac.kr`, and Donald's is `trump@wh.com`. Fill the blanks below to describe what happens in the delivery of the email. Assume that Donald's computer talks directly to Kim's SMTP server.

A. The resolver in Donald's email program first looks up the resolver cache on Donald's computer. (Hint: this table can be displayed by `ipconfig/displaydns` on Windows.)

B. The lookup in (A) fails to find a matching entry. The resolver, as a next resort, sends the default name server a query with Type = A and Query name = korea.ac.kr.

C. The default name server does not have the resource record in its cache, either, so it queries a root name server (Hint: There are only 13 of these in the world.)

D. After a complicated chain of queries and responses exchanged between name servers, the default name server finally provides the DNS response to the resolver. In particular, the IP address of the mail server for korea.ac.kr domain is 163.152.6.22.

E. Using the IP address, Donald's mail program sets up a TCP connection to port 25 of the computer with the IP address.

F. When the IP datagram carrying the TCP segment reaches the routing table, two output values are obtained. They are next hop IP address and the outgoing interface.

G. The outgoing interface happens to be Ethernet. So ARP cache lookup takes place. The answer of (F) is carried in the target protocol address field of the ARP request, so that every SMTP message encapsulated in TCP segment that is in turn encapsulated in IP datagram is carried in Ethernet frame goes through the interface with this IP address.

H. The answer obtained in the ARP transaction is the Ethernet address corresponding to the next hop IP address.

I. In the 3-way handshake the SMTP server at `korea.ac.kr`, Donald's computer provides ISN, window size, and MSS, for synchronizing with the server, among which MSS is in the options field.

J. The MSS specified in the SYN segment is 1460 bytes.

K. Once the connection is successfully set up, the SMTP server at `camel.edu` provides the return code of 220.

L. Donald's email was very short, only containing this single line: "I am your father." Write down the sequence of SMTP messages that Donald's email program sends to the SMTP server at `korea.ac.kr` domain, in order to send the above simple mail. Assume Donald's computer has the domain name `twit.wh.com`. **[5pts].**

HELO twit.wh.com

MAIL FROM: trump@wh.com

RCPT TO: kimj@korea.ac.kr

DATA I am you father.

.

M. Suppose the SMTP server at `korea.ac.kr` doubles as a POP3 server, and Kim uses POP3 to retrieve her mail there. If Donald's mail is the only one in Kim's mail box, how would Kim's POP3 mail reader talk to the POP3 server to retrieve Donald's mail? Assuming the TCP connection has been already set up to the POP3 server, write down the three input lines that Kim's computer needs to provide, given Kim's password for the email account is "`cvid`." **[3pts]**

user kimj

pass cvid

retr 1

4. Answer the questions about the following trace for a DNS query for `korea.ac.kr` made through the `nslookup` program.

   A. In packet #13, why would the resolver try to look up the apparently absurd domain name `korea.ac.kr.korea.ac.kr`? (Hint: "suffix") **[4pts]** **The resolver was configured to attach korea.ac.kr as suffix in case the query name is not a FQDN.**

   B. In the given condition that would cause the problem in (A), what domain name as the query name would you use to prevent the useless lookup? Precisely write the domain name (1 character per box). **[1pt]**

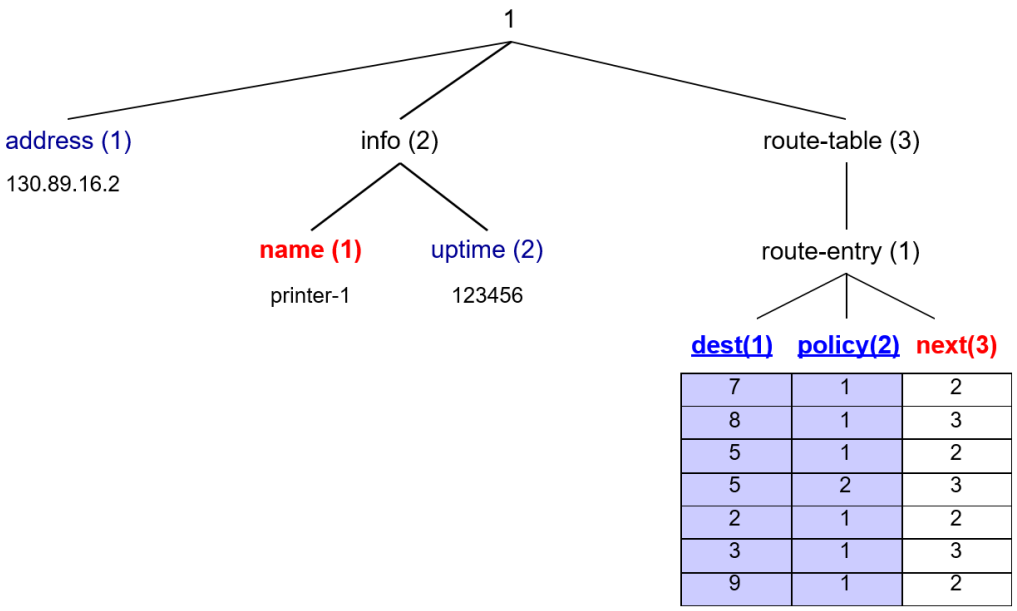
k	**o**	**r**	**e**	**a**	**.**	**a**	**c**	**.**	**k**	**r**	**.**			

   C. What does packet #16 tell us? (Hint: RR type AAAA is "IPv6 address.") **[2pts]** korea.ac.kr doesn't have an IPv6 address associated with it

   D. What is the transaction ID of the DNS packet that contains the desired answer? **[1pt]** 0x0008

```
13 2.546969   192.168.0.11   163.152.1.1     DNS      83 Standard query 0x0006 A korea.ac.kr.korea.ac.kr
14 2.561634   163.152.1.1    192.168.0.11    DNS     131 Standard query response 0x0006 No such name A korea.ac.kr.k
15 2.562042   192.168.0.11   163.152.1.1     DNS      83 Standard query 0x0007 AAAA korea.ac.kr.korea.ac.kr
16 2.568141   163.152.1.1    192.168.0.11    DNS     131 Standard query response 0x0007 No such name AAAA korea.ac.k
17 2.568448   192.168.0.11   163.152.1.1     DNS      71 Standard query 0x0008 A korea.ac.kr
18 2.572930   163.152.1.1    192.168.0.11    DNS     159 Standard query response 0x0008 A korea.ac.kr A 163.152.6.10
```

5. Answer the questions regarding the following OID tree.



   A. Write down the object name to get the argument of a GetRequest for the uptime value. 1.2.2.0 **[1pt]**

   B. What is the value that you would get if you used GetNextRequest instead using the same argument? **[2pts]** 2

C. What is the value that you will get if you issue another GetNextRequest using the answer to (B) for the argument of the request? **[2pts]** 3

D. Specify the index column(s) for the routing table. Columns 1 & 2 **[1pt]**

E. What is the reason that SNMP uses the "index value" instead of the "row number" to access a value in a table? Table entries can be dynamically added and deleted – we probably do not know where the wanted entry is. **[2pts]**

6. Suppose a variable binding in a SNMP GetResponse is `30 14 06 0a 2b 06 01 02 01 02 02 01 06 01 04 06 08 00 37 15 eb bc`. (Hint: use the following table to decode the binding.)

A. What is the object name of the variable? 1.3.6.1.2.1.2.2.1.6.1 **[2pts]**

B. What is its value returned by the SNMP agent? 08 00 37 15 eb bc (in hexadecimal) **[2pt]**

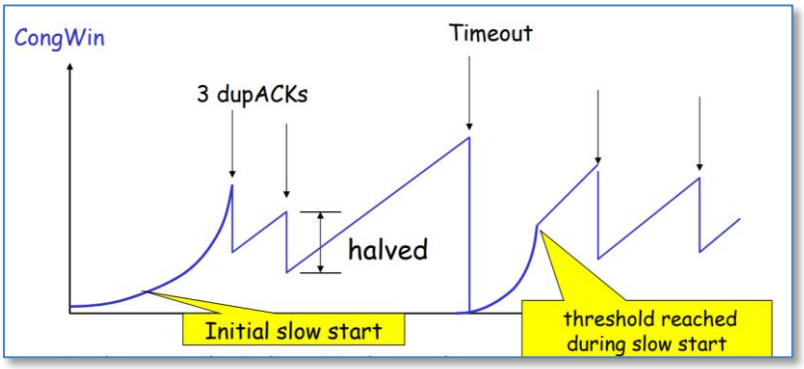
C. What is the data type of the value? Octet string **[1pt]**

Data Type	*Tag (Hex)*	*Data Type*	*Tag (Hex)*
INTEGER	**02**	IPAddress	**40**
OCTET STRING	**04**	Counter	**41**
OBJECT IDENTIFIER	**06**	Gauge	**42**
NULL	**05**	TimeTicks	**43**
SEQUENCE, SEQUENCE OF	**30**	Opaque	**44**

7. The following figure depicts how TCP congestion window size ("CongWin") is controlled. The exponential increase is caused by the "Slow Start" algorithm, whereas the linear increase is caused by the "Congestion Avoidance" algorithm. Both are implemented in a single line in the TCP code. Fill in the blanks with a constant or with an expression.

A. Slow Start: CongWin ← CongWin + 1 (MSS) **[2pts]**

B. Congestion Avoidance: CongWin ← CongWin + 1/CongWin (MSS) **[3pts]**



8. There are two ways to make a multicast router listen to IGMP messages. What are they?

A. Set the Router Alert option (Hint: IP option) **[3pts]**

B. Let them implicitly join all multicast groups **[2pts]**

9. In IGMPv2, an end host that has been subscribing 233.18.158.61 is leaving the group. What is the destination IP address? 224.0.0.2 **[2pts]**

10. In IGMPv3, an end host decides to join a group without excluding any source.

A. What is the mode? CHANGE-to-EXCLUDE **[2pts]**

B. What is the set of sources it specifies in the group membership report? Empty set **[1pt]**

11. Answer the following question on the TCP trace shown below.

A. What are the option(s) that this TCP connection will use? MSS, SACK **[4pts]**

B. What kind of service does the server provide to the client? Email (or SMTP) **[1pt]**

C. In which data segment is the Nagle algorithm taking effect? Write down the relevant segment numbers. 10,12,14,16,18,20,22,24,26 **[3pts]**

D. How many data bytes were carried by packet #4? 50 bytes **[4pts]**

1	192.168.0.11	148.163.149.48	66	4780 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	148.163.149.48	192.168.0.11	62	25 → 4780 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
3	192.168.0.11	148.163.149.48	54	4780 → 25 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	148.163.149.48	192.168.0.11	104	S: 220 mx0a-000c6b02.pphosted.com ESMTP pe-m0100506
5	192.168.0.11	148.163.149.48	54	4780 → 25 [ACK] Seq=1 Ack=51 Win=64190 Len=0
6	192.168.0.11	148.163.149.48	55	4780 → 25 [PSH, ACK] Seq=1 Ack=51 Win=64190 Len=1 [TCP segment of a re
7	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=2 Win=4381 Len=0
8	192.168.0.11	148.163.149.48	55	4780 → 25 [PSH, ACK] Seq=2 Ack=51 Win=64190 Len=1 [TCP segment of a re
9	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=3 Win=4382 Len=0
10	192.168.0.11	148.163.149.48	62	4780 → 25 [PSH, ACK] Seq=3 Ack=51 Win=64190 Len=8 [TCP segment of a re
11	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=11 Win=4390 Len=0
12	192.168.0.11	148.163.149.48	57	4780 → 25 [PSH, ACK] Seq=11 Ack=51 Win=64190 Len=3 [TCP segment of a r
13	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=14 Win=4393 Len=0
14	192.168.0.11	148.163.149.48	66	4780 → 25 [PSH, ACK] Seq=14 Ack=51 Win=64190 Len=12 [TCP segment of a
15	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=26 Win=4405 Len=0
16	192.168.0.11	148.163.149.48	58	4780 → 25 [PSH, ACK] Seq=26 Ack=51 Win=64190 Len=4 [TCP segment of a r
17	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=30 Win=4409 Len=0
18	192.168.0.11	148.163.149.48	67	4780 → 25 [PSH, ACK] Seq=30 Ack=51 Win=64190 Len=13 [TCP segment of a
19	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=43 Win=4422 Len=0
20	192.168.0.11	148.163.149.48	57	4780 → 25 [PSH, ACK] Seq=43 Ack=51 Win=64190 Len=3 [TCP segment of a r
21	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=46 Win=4425 Len=0
22	192.168.0.11	148.163.149.48	68	4780 → 25 [PSH, ACK] Seq=46 Ack=51 Win=64190 Len=14 [TCP segment of a
23	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=60 Win=4439 Len=0
24	192.168.0.11	148.163.149.48	58	4780 → 25 [PSH, ACK] Seq=60 Ack=51 Win=64190 Len=4 [TCP segment of a r
25	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=64 Win=4443 Len=0
26	192.168.0.11	148.163.149.48	62	4780 → 25 [PSH, ACK] Seq=64 Ack=51 Win=64190 Len=8 [TCP segment of a r
27	148.163.149.48	192.168.0.11	54	25 → 4780 [ACK] Seq=51 Ack=72 Win=4451 Len=0
28	192.168.0.11	148.163.149.48	56	C: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
29	148.163.149.48	192.168.0.11	161	S: 500 5.5.1 Command unrecognized: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

12. The following is the output from `netstat` command executed at `192.169.0.11`.

A. How many connections are eligible for data exchange in both directions? 4 **[2pts]**

B. In how many connections did the remote machine send the first FIN segment? 4 **[3pts]**

TCP	192.168.0.11:4994	54.192.183.9:443	CLOSE_WAIT
TCP	192.168.0.11:4998	52.230.7.59:443	ESTABLISHED
TCP	192.168.0.11:4999	52.85.122.105:443	CLOSE_WAIT
TCP	192.168.0.11:5000	113.29.138.231:443	ESTABLISHED
TCP	192.168.0.11:5001	54.192.183.24:443	CLOSE_WAIT
TCP	192.168.0.11:5014	74.125.204.188:443	ESTABLISHED
TCP	192.168.0.11:5567	108.177.97.189:443	ESTABLISHED
TCP	192.168.0.11:5702	117.18.232.200:443	CLOSE_WAIT
TCP	192.168.0.11:5720	180.87.4.149:443	TIME_WAIT
TCP	192.168.0.11:5721	180.87.4.149:443	TIME_WAIT

13. In the following figure, each square represents a single segment of size MSS. Let us call the number in the square the "packet number," for our convenience. Assuming that the send data stream and the receive data stream are perfectly aligned in the figure (*i.e.*, "0" at P1 is "0" at P2), answer the following questions:

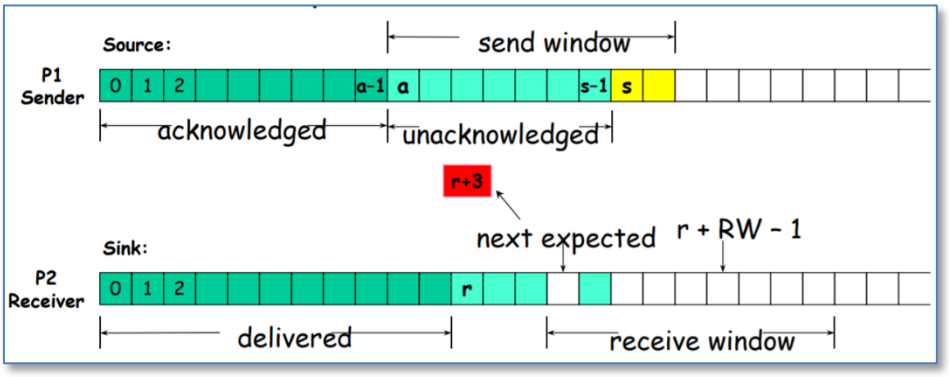
A. Up to which packet can P1 flush from the send socket buffer? Write down its "packet number". a-1 **[2pts]**

B. How many non-duplicate ACKs will P1 receive further if the situation depicted in the figure remains the same? 5 **[2pts]**

C. Up to which packets can the application at P2 use? Write down the "packet number" of the last packet delivered to the application. r+2 **[2pts]**

D. Would the depicted situation trigger the Fast Retransmit algorithm at P1? (Y/N) N **[1pt]** Briefly explain why (or why not). **[2pts]** Only one duplicate ACK has been triggered by r+4

E. In the duplicate ACK for $r + 3$, what value would the header length field have (in hexadecimal) in the TCP header if SACK is the only option used in the ACK segment? 0x8 **[3pts]**



14. Select the right action from (1)-(4) for each given event at the TCP receiver. **[4pts]**

Event at Receiver	Action
Arrival of in-order segment with expected seq #. All data up to expected seq # already ACKed	(2)
Arrival of in-order segment with expected seq #. One other segment has ACK pending	(1)
Arrival of out-of-order segment higher-than-expect seq. # . Gap detected	(4)
Arrival of segment that partially or completely fills gap	(3)

(1) Immediately send single cumulative ACK, ACKing both in-order segments
(2) Delayed ACK. Wait up to 200 ms for next segment. If no next segment, send ACK.
(3) Immediately send ACK, provided that segment starts at lower end of gap
(4) Immediately send duplicate ACK, indicating sequence number of next expected byte

15. Verify the following statements by marking "T" (true) or "F" (false). **[4pts]**

Statement	**T/F**
Between user and mail transfer agent, SMTP pushes and pulls emails.	F
In some cases, TCP can send beyond the right edge of the sending window.	T
When TCP Persist timer runs, there are no outstanding segments.	T
In TCP, the probability that a RTT exceeds the RTO is less than 4%.	F