# 인터넷 프로토콜 2019 기말고사 답안지

학번 _____ 이름 _____

**!!!모든 전자기기 사용 금지!!!** **시험 시간: 1 시간**

1. 공유형 링크로 인터넷에 연결된 호스트로부터 어떤 서버로 패킷이 보내질 때, 일어나는 다음의 번역 과정에서 밑줄 쳐진 빈 괄호 안을 메워라. ( )괄호 안은 프로토콜 혹은 처리 과정이며 [ ] 괄호 안은 정보의 형태이다.

   A [서버 도메인이름] → (_____DNS_____) → [최종목적지 IP주소]→ (라우팅 테이블 조회) → [___다음 홉 IP 주소_____] → (_____ARP_____) → [다음 홉 MAC 주소] **[각 1점]**

2. 다음 주장 중 일반적으로 성립하는 것에는 O, 그렇지 않은 것에는 X를 하라 **[각 1점]**

   A A 타입 RR은 PTR RR과 1:1 대응한다 X
   B SNMP의 inform 요청은 trap과는 달리 수신자로부터 확인을 받는다. O
   C 한글 레이블이 DNS에 쓰이려면 영문자/기호/숫자 63자 이내의 레이블로 번역되어야 한다 O
   D TCP에서는 data 세그먼트만 재전송될 수 있고 ACK 세그먼트는 재전송되지 않는다 O
   E 응용이 공급한 도메인 이름을 FQDN으로 만들어 주는 주체는 리졸버이다 O
   F SNMP MIB은 원래 agent 내에 존재한다. X
   G NS RR 타입도 round-robin DNS의 대상이다 O
   H 224.0.0.0/24 주소들은 link local로만 쓸 수 있다 O
   I Root name server의 replication을 위해서는 anycast 기술이 사용된다. O
   J TCP에서 out-of-order로 도착한 세그먼트들은 reordering buffer에 임시 저장한다 O
   K Korea.ac.kr 도메인의 zone file 원본을 가진 서버를 알기 위해서는 query type을 NS로 설정해야 한다 X
   L TCP sender의 send window의 오른쪽 경계를 넘어 데이터 바이트를 전송할 수 있는 경우는 오직 persist timer가 expire된 경우 뿐이다 O
   M SNMP 메시지 중 여러 variable-value binding이 있을 때 이 중에 여러 개가 에러를 발생시켰다면 error index는 그 중 맨 첫 pair의 번호이다. O
   N PIM dense mode에서는 RPF check를 위해 별도의 라우팅 테이블이 필요하다. X
   O TCP Delayed ACK 알고리듬을 사용하면 2개의 데이터 세그먼트마다 1개의 ACK가 전송된다. X

3. TCP 수신자가 다음에 받을 것으로 기대하는 시퀀스 번호를 EXP라고 하고, 이 때 도착하는 세그먼트의 시퀀스 번호를 SEQ라고 할 때, 수신측 TCP의 반응은 delayed ACK, duplicate ACK, immediate ACK 중 하나가 될 수 있다. 다음 각 경우에 이 중 하나를 골라 적고, 간단히 이유를 설명하라. **[각 1점]**

   A SEQ > EXP: duplicate ACK: cumulative ACK 때문이다
   B SEQ = EXP: delayed ACK: TCP 수신자는 기본적으로 ACK를 지연시킨다
   C SEQ < EXP: immediate ACK: 이미 받은 시퀀스 번호에 대해 TCP 전송자에게 즉각 경고한다

4. IPTV에 IP 멀티캐스트를 사용할 때, 멀티캐스트 라우팅 프로토콜로 PIM-DM이 바람직하지 못한 것은 무슨 이유 때문인가? 시청률과 연관지어 설명하라. **[2점]** 시청하지 않는 가입자에게까지 주기적으로 멀티캐스트 패킷이 flooding 되기 때문이다 (OR) 결국 대부분 pruning할 Multicast tree 를 비효율적으로 만들기 때문이다

5. SNMP에 대한 다음 질문에 답하라.

   A 에이전트가 매니저로부터 메시지를 받기 위해 사용하는 포트 번호는? 161 **[1점]**
   B 매니저가 에이전트로부터 메시지를 받기 위해 사용하는 포트 번호는? 162 **[1점]**
   C SNMP는 왜 트랜스포트로 TCP가 아닌 UDP를 사용하는가? TCP를 사용하면 TCP 연결이 끊어지면서 SNMP 패킷의 배달이 fault에 의해 장애를 받기 때문이다. (OR) UDP 데이터그램은 fault를 우회하여 전달되기 때문이다 **[3점]** (힌트: 네트워크 관리에는 fault management가 포함된다)

6. 다음은 어느 호스트가 DNS로부터 받은 응답이다.

   A 이 호스트는 gms.ahnlab.com의 A 타입 RR을 요구했다. 그런데 응답에는 이 도메인 이름에 대한 IP 주소는 나타나지 않는다. 대신 DNS는 CNAME 타입의 RR을 답으로 주었다. 이유가 무엇이겠는가? **[3점]** gms.ahnlab.com은 A 타입 RR이 없고 대신 CNAME RR 밖에 없기 때문이다

   B DNS는 답과 더불어 gms.wip.ahnlab.com의 네임 서버 정보도 주었다. 만일 이 호스트가 다음에 gms.wip.ahnlab.com에 대해 질문할 때 어떤 이득이 있는가? Root name server 등 DNS의 높은 hierarchy에 있는 서버들과 연관하여, 그리고 캐쉬에서 응답을 얻을 수 없다는 전제 하에 답하라. **[3점]** Root name server 등 높은 hierarchy에 있는 서버들을 거치지 않고 직접 gtm2[1].ahnlab.com에게 query를 던질 수 있으므로 효율적이다 (OR) 같은 이유로 속도가 빠르다

```
▾ Queries
  › gms.ahnlab.com: type A, class IN
▾ Answers
  › gms.ahnlab.com: type CNAME, class IN, cname gms.wip.ahnlab.com
  › gms.wip.ahnlab.com: type A, class IN, addr 211.115.106.74
▾ Authoritative nameservers
  › gms.wip.ahnlab.com: type NS, class IN, ns gtm2.ahnlab.com
  › gms.wip.ahnlab.com: type NS, class IN, ns gtm1.ahnlab.com
```

7. TCP keepalive probe(KP)와 persist probe(PP)의 차이점 3가지를 간략히 적어라

   A (데이터 적재 여부) KP: NO PP:YES **[각 1점]**

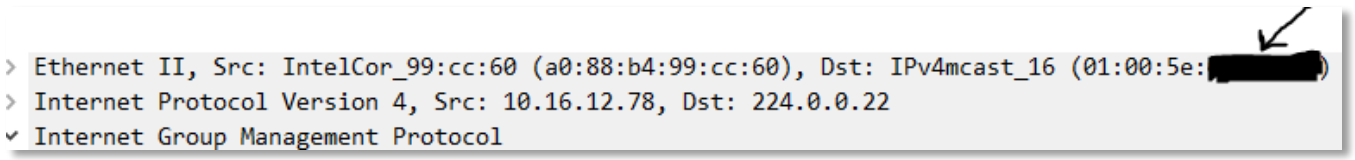
   B (sequence 번호 특징) KP: SEQ < EXP PP: SEQ = EXP **[각 2점]**

   C (보내는 상황) KP: 상대방 TCP가 살아 있나를 확인할 때 (OR) half-open 상태인지 확인할 때
   PP: TCP 수신자의 receive socket buffer가 아직도 꽉 찬 상태인지 테스트할 때 **[각 2점]**

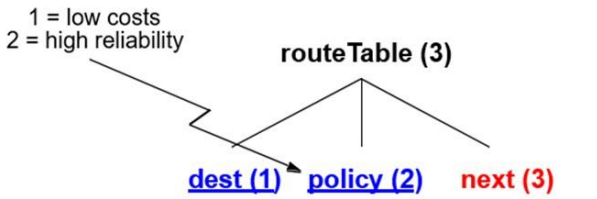
8. 한글 표기를 위해 참고사용한 UTF-8 방식에서 '가' = 0xeab080 이다. 이 때, '가'를 이메일 메시지에 적었다면 base-64 인코딩을 사용한 MIME 방식에서는 어떤 문자열로 표현되는가? 아래 base-64 테이블을 참고하라. 6rCA **[3점]**

| Value | Char | Value | Char | Value | Char | Value | Char |
|---|---|---|---|---|---|---|---|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |

9. 아래 그림에서 화살표가 가리키는 부분에 들어갈 3 바이트 값을 hexadecimal로 적어라. 00:00:16 **[1점]**



10. 다음 라우팅 테이블이 있다고 하자. 왼쪽 두 칼럼이 함께 인덱스로 쓰이고 있다. 이 때,




| | | |
|---|---|---|
| 130.89.16.23 | 2 | 130.89.16.33 |
| 130.89.16.23 | 1 | 130.89.16.23 |
| 130.89.19.121 | 1 | 130.89.16.1 |
| 19.1.23.24 | 2 | 130.89.16.1 |
| 19.1.23.24 | 1 | 130.89.16.4 |
| 19.1.11.97 | 1 | 130.89.16.1 |

A Get-next(3.3.19.1.23.24.2)의 결과로 agent가 보고할 값은 얼마인가? **[3점]** 130.89.16.23

B Get-bulk(3.1; max-repetitions=2)의 결과로 agent가 보고할 값들은 무엇인가? 19.1.11.97, 19.1.23,24 **[2점]**

| *Type* | *Tag (Hex)* | *Type* | *Tag (Hex)* |
|---|---|---|---|
| GetRequest | **A0** | GetBulkRequest | **A5** |
| GetNextRequest | **A1** | InformRequest | **A6** |
| Response | **A2** | Trap (SNMPv2) | **A7** |
| SetRequest | **A3** | Report | **A8** |

| *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** |

11. 윈도우 시스템에서 Resolver cache의 내용을 보기 위한 명령은 무엇인가? Ipconfig/displaydns
Resolver cache의 내용을 모두 지우기 위한 명령은 무엇인가? Ipconfig/flushdns **[각 1점]**

12. 위에 있는 두 표를 참고하여, BER 인코딩을 써서 UDP 데이터그램 안에 다음과 같이 표현된 SNMP 메시지를 해독하라.

A SNMP 버전 = 1 **[1점]**

B Community string = public (소문자) (힌트: ASCII 값 'a' = 0x61) **[2점]**

C PDU 종류 = get (OR) GetRequest **[1점]**

D Request ID = 38 (OR) 0x26 **[1점]**

E 사용된 object ID = 1.3.6.1.2.1.1.2.253 **[3점]**

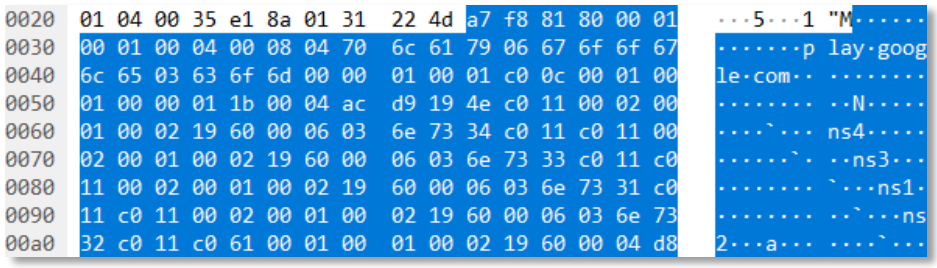
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 30 | 27 | 02 | 01 | 00 | 04 | 06 | 70 |
| 75 | 62 | 6c | 69 | 63 | a0 | 1a | 02 |
| 01 | 26 | 02 | 01 | 00 | 02 | 01 | 00 |
| 30 | 0f | 30 | 0d | 06 | 09 | 2b | 06 |
| 01 | 02 | 01 | 01 | 02 | 81 | 7d | 05 |
| 00 | | | | | | | |

13. 아래에서 하이라이트가 된 부분은 DNS 패킷이다. DNS 메시지 안에서 google.com이란 도메인 이름이 두 번째로 쓰일 때, 다음 질문에 답하라. (힌트: DNS 헤더는 12 바이트이다)

A 이 두 번째 등장한 google.com은 몇 바이트로 표현되는가? 2 **[1점]**

B 그 값은 16진수로 무엇인가? C0 11 **[3점]**

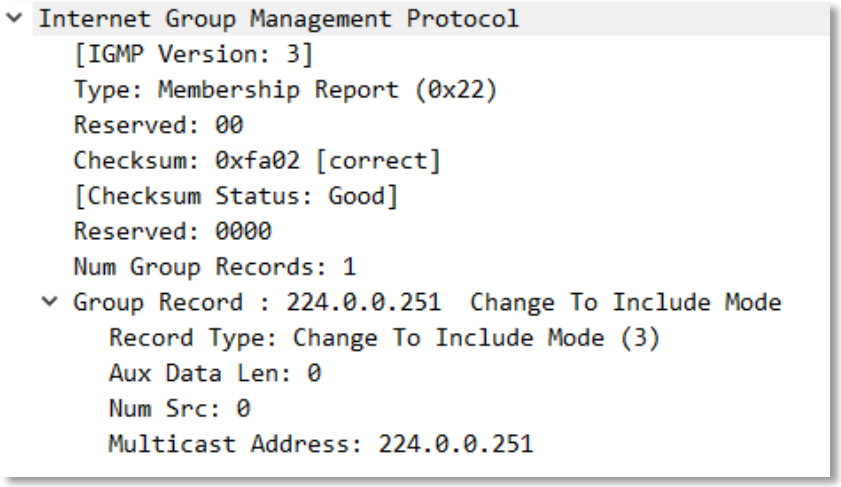
C DNS가 이런 일을 하는 취지는? 512 바이트로 제한된 DNS 패킷 크기를 넘기지 않기 위해 최대한 길이를 줄이려고 **[2점]**




14. 다음은 IGMPv3 메시지이다. 다음 질문에 답하라. (힌트: 전송자(source) 정보에 주의하라)

A 어떤 의도로 보내진 메시지인가? 그룹 탈퇴 (leave) **[2점]**

B 그 의도를 알 수 있는 값은 무엇인가? Num Src 0 **[2점]**




15. 아래는 telnet mx1.hanmail.net 25를 수행하자 마자 "QUIT"와 Enter 키(CR+LF)를 누른 결과이다.

A 이 연결에서 내 컴퓨터가 보내는 FIN 세그먼트의 시퀀스 번호는 최초 시퀀스 번호보다 몇 큰가? 7 **[3점]**

B 첫 번째 FIN을 내 컴퓨터가 아닌 mx1.hanmail.net이 먼저 보낸다고 할 때, 어느 쪽이 TCP 연결 상태를 더 늦게까지 유지해야 하는가? Mx1.hanmail.net **[1점]** 왜인가? 마지막 ACK를 보내게 되어 TIME_WAIT 상태에서 상대편에서 올지 모를 FIN 재전송을 기다려야 하므로 **[2점]**




16. TCP "연결"을 규정하는 3개의 숫자는 두 개의 데이터 채널에 대해 각각 정의된다.

A 이 때, TCP 고정 헤더에 들어가지 않고 옵션에 들어가는 값은 무엇인가? MSS **[1점]**

B 양 데이터 채널에서 결국 하나의 값으로 통일되는 것은 무엇인가? MSS **[1점]**

17. 아래에서 맺어진 TCP 연결에서 211.231.108.46이 TCP 고정 헤더의 window 크기 필드에 0x001d 라고 적어서 보냈다. 211.231.108.46의 receive socket buffer의 실제 크기는 얼마인가? 29696 **[2점]**

| Source | Destination | Info |
|---|---|---|
| 172.30.1.4 | 211.231.108.46 | 55162 → 25 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 211.231.108.46 | 172.30.1.4 | 25 → 55162 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024 |

18. 다음은 어느 TCP acknowledgement에 나타난 SACK 옵션 부분이다.

A 왜 두 개의 NOP 옵션이 필요한가? TCP 시퀀스 번호의 크기와 관련해서 설명하라 시퀀스번호 4개 * 4 = 16 바이트 + SACK 옵션 type 1 바이트 + length 1바이트 = total 18 바이트. 4 바이트 align을 위해 2 NOP (각 1 바이트) 필요 **[2점]**

B TCP 수신자가 불연속으로 받은 바이트의 개수는 총 몇 개인가? 93901 **[3점]**

```
▾ Options: (20 bytes), No-Operation (NOP), No-Operation (NOP), SACK
  › TCP Option - No-Operation (NOP)
  › TCP Option - No-Operation (NOP)
  › TCP Option - SACK 1368822-1455571 1354522-1361672
```

19. Nagle 알고리듬을 테스트하기 위해 (1) mx1.hanmail.net과 (2) MIT의 메일 서버인 mit-edu.mail.protection.outlook.com의 25번 포트에 각각 연결한 뒤 자판에서 "." 키를 누른 상태에서 30초간 떼지 않았다.

A 어느 쪽에서 Nagle 알고리듬이 효과적일까? MIT **[1점]**

B 이유는 무엇인가? RTT가 커서 이전 small segment에 대한 ACK가 돌아오기까지 동안 send socket buffer에 "." 글자를 많이 모을 수 있기 때문이다 **[2점]**

C Wireshark에서 이 두 TCP 연결에 흐르는 TCP 세그먼트들에 대해 무엇을 관찰해 보면 (A)에서 내린 결론을 확인할 수 있는가? 시퀀스 번호 증가 크기 (OR) ACK 번호 증가 크기 **[2점]**

20. 다음 그림은 TCP sender의 바이트 스트림 상태를 보이고 있다. 현실과는 거리가 멀지만, 각 숫자는 바이트 시퀀스 번호라고 가정하라.

A 이 TCP sender가 마지막으로 받은 ACK 번호는 무엇이었나? 4 **[2점]**

B 그 ACK 세그먼트에 쓰인 window 값은 얼마였는가? 5 **[1점]**

C 그 ACK를 보낸 뒤 수신측 응용이 2 바이트를 읽었다고 하자. 그 결과로 수신측 receive socket buffer에는 몇 바이트의 빈 공간이 남게 되었는가? 4 **[1점]**

