

과제 04 수행보고서

정보통신공학전공

200301582

김성태

과제 수행 목적 & 과제 내용

- SimTL 분석 모듈 추가
 - CSMA/SD 디코더 개발
 - 요약 파일에 발착신 MAC 주소 추가
 - 감시한 프레임에 대해 CSMA/CD 프로토콜을 분석하여 해당 파일에 기입 .
 - SimTL 의 수행결과를 Wireshark 와 비교하여 제대로 개발되었는지를 확인 .

주요 모듈 설명

- `if(p_option->eflag) { // eflag 를 확인`
- `for(j = 0; j < ETH_ALEN; j++) {`
- `fprintf(fd_tmp, "%X", ep->ether_dhost[j]);`
- `if(j != 5) {`
- `fprintf(fd_tmp, " : ");`
- `}}`
- `for(j = 0; j < ETH_ALEN; j++) {`
- `fprintf(fd_tmp, "%X", ep->ether_shost[j]);`
- `if(j != 5) {`
- `fprintf(fd_tmp, " : ");`
- `}}`
- `fprintf(fd_tmp, "\n\tether_type -> %x\n",`
`ntohs(ep->ether_type));`
- `}`

- 옵션 확인 후
- 해당 필드에 맞는 정보를 알맞게 뿌려준다 .
- `ether_type` 필드는 네트워크 바이트 순서 (Network Byte Order) 로 되어있으므로 유의 해야 한다 .
- 네트워크 순서는 빅 - 인디언 (Big-Endian) 방식이다 .
- 이를 `ntohs()` 함수를 통해 리틀 - 인디언 (Little-Endian) 순서로 바꾸어 주어 나타낸다 .

실행화면

```
pchero@MyNote: ~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/04/SimTL/test
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote: ~/Desktop/Study/REPORT/pr... 2008.4.28_2:22:51.381718 = (/tmp/SimTL) -... ethernet.h = (/usr/include/net) - VIM pchero@MyNote: ~/Desktop
8: /tmp/SimTL/2008.4.28_2:19:50.81792 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
10.125.213.93 Version:4 Header_Length:5 Service:0 Total_Length:52
9: /tmp/SimTL/2008.4.28_2:19:50.83000 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
10.125.213.93 Version:4 Header_Length:5 Service:0 Total_Length:52
Do you want a Save? [Y/n] :n
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/04/SimTL$ sudo ./SimTL_beta "src host 192.168.10.110 and
tcp port 80" -i eth0 -c 10 -e -p
device = eth0
0: /tmp/SimTL/2008.4.28_2:22:51.381718 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.231.51.49 Version:4 Header_Length:5 Service:0 Total_Length:52
1: /tmp/SimTL/2008.4.28_2:22:59.867867 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.231.51.49 Version:4 Header_Length:5 Service:0 Total_Length:52
2: /tmp/SimTL/2008.4.28_2:25:3.108556 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
11.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:60
3: /tmp/SimTL/2008.4.28_2:25:3.122666 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
11.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:52
4: /tmp/SimTL/2008.4.28_2:25:3.122845 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
11.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:614
5: /tmp/SimTL/2008.4.28_2:25:3.137560 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
11.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:52
6: /tmp/SimTL/2008.4.28_2:25:46.99751 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:60
7: /tmp/SimTL/2008.4.28_2:25:46.109488 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:40
8: /tmp/SimTL/2008.4.28_2:25:46.141018 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:527
9: /tmp/SimTL/2008.4.28_2:25:46.182517 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74 IP:: 192.168.10.110----->2
22.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:40
Do you want a Save? [Y/n] :y
Type the save path.
Dir : ./test
/bin/cp -f /tmp/SimTL/* ./testpchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/04/SimTL$ cd test/
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/04/SimTL/test$ ls
2008.4.28_1:42:15.788407 2008.4.28_1:42:15.843384 2008.4.28_1:42:15.876475 2008.4.28_2:25:3.108556 2008.4.28_2:25:46.109488  traceManager
2008.4.28_1:42:15.796190 2008.4.28_1:42:15.844536 2008.4.28_1:42:16.19682 2008.4.28_2:25:3.122666 2008.4.28_2:25:46.141018
2008.4.28_1:42:15.833033 2008.4.28_1:42:15.858884 2008.4.28_2:22:51.381718 2008.4.28_2:25:3.122845 2008.4.28_2:25:46.182517
2008.4.28_1:42:15.834254 2008.4.28_1:42:15.859243 2008.4.28_2:22:59.867867 2008.4.28_2:25:3.137560 2008.4.28_2:25:46.99751
pchero@MyNote:~/Desktop/Study/REPORT/profe.kimtj/Internet_Engineering/04/SimTL/test$
```

실행화면 - 요약파일

```
pchero@MyNote: /tmp/SimTL
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote: ~/Desktop/Study/REPORT/pr... x pchero@MyNote: /tmp/SimTL x ethernet.h = (/usr/include/net) - VIM x pchero@MyNote: ~/Desktop x
pchero@MyNote: /tmp/SimTL$ cat
2008.4.28_2:22:51.381718 2008.4.28_2:25:3.108556 2008.4.28_2:25:3.122845 2008.4.28_2:25:46.109488 2008.4.28_2:25:46.182517 t raceManager
2008.4.28_2:22:59.867867 2008.4.28_2:25:3.122666 2008.4.28_2:25:3.137560 2008.4.28_2:25:46.141018 2008.4.28_2:25:46.99751
pchero@MyNote: /tmp/SimTL$ cat traceManager
1: /tmp/SimTL/2008.4.28_2:22:51.381718 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.231.51.49 Version:4 Header_Length:5 Service:0 Total_Length:52
2: /tmp/SimTL/2008.4.28_2:22:59.867867 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.231.51.49 Version:4 Header_Length:5 Service:0 Total_Length:52
3: /tmp/SimTL/2008.4.28_2:25:3.108556 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->211.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:60
4: /tmp/SimTL/2008.4.28_2:25:3.122666 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->211.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:52
5: /tmp/SimTL/2008.4.28_2:25:3.122845 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->211.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:614
6: /tmp/SimTL/2008.4.28_2:25:3.137560 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->211.115.116.100 Version:4 Header_Length:5 Service:0 Total_Length:52
7: /tmp/SimTL/2008.4.28_2:25:46.99751 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:60
8: /tmp/SimTL/2008.4.28_2:25:46.109488 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:40
9: /tmp/SimTL/2008.4.28_2:25:46.141018 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:527
10: /tmp/SimTL/2008.4.28_2:25:46.182517 0 : 50 : 18 : 19 : 66 : C -----> 0 : 14 : 22 : 9A : 53 : 74
   ether_type -> 800
   IP:: 192.168.10.110----->222.122.237.240 Version:4 Header_Length:5 Service:0 Total_Length:40
pchero@MyNote: /tmp/SimTL$
```

실행화면 - Wireshark 비교

2008.4.28_2:22:51.381718 = (//tmp/SimTL) - VIM

```

===== DataLink Layer =====
0 : 50 : 18 : 19 : 66 : C ----> 0 : 14 : 22 : 9A : 53 : 74
ether_type -> 800

===== IP HEADER =====
192.168.10.110 ----> 222.231.51.49
Version : 4
Header Length : 5
Service : 0
Total Length : 52
Identification : 28294
Fragment Offset : 16384
Time to Live : 64
Checksum : 61198

===== TCP HEADER =====
Source Port : 57643
Destination Port : 80
Sequence Number : 4193663393
Acknowledgement Number : 634055566
Data Offset : 8
Window : 1136
URG : 0 ACK : 1 PSH : 0 RST : 0 SYN : 0 FIN : 0

===== TCP DATA(HEXA) =====
===== TCP DATA(CHAR) =====

<<<<<<<<<<<< End of Data >>>>>>>>>>
    
```

1,0-1 모두

eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression...

No.	Time	Source	Destination	Protocol	Info
1401	301.191732	192.168.10.110	222.231.51.49	TCP	51912 > http [F]
1402	405.551174	192.168.10.110	211.115.116.100	TCP	45878 > http [A]
1403	406.185527	192.168.10.110	211.115.116.100	TCP	45878 > http [F]
1404	442.699173	192.168.10.110	222.231.51.49	TCP	57643 > http [A]
1405	451.185480	192.168.10.110	222.231.51.49	TCP	57643 > http [F]

▸ Frame 1404 (66 bytes on wire, 66 bytes captured)
 ▾ Ethernet II, Src: Dell_9a:53:74 (00:14:22:9a:53:74), Dst: Amit_19:66:0c (00:50:18:19:66:0c)
 ▸ Destination: Amit_19:66:0c (00:50:18:19:66:0c)
 ▸ Source: Dell_9a:53:74 (00:14:22:9a:53:74)
 Type: IP (0x0800)
 ▸ Internet Protocol, Src: 192.168.10.110 (192.168.10.110), Dst: 222.231.51.49 (222.231.51.49)
 ▸ Transmission Control Protocol, Src Port: 57643 (57643), Dst Port: http (80), Seq: 2862, Ack: 369156, Len: 0

```

0000 00 50 18 19 66 0c 00 14 22 9a 53 74 08 00 45 00  .p.f.. ".St..E.
0010 00 34 6e 86 40 00 40 06 ef 0e c0 a8 0a 6e de e7  .4n.@. ....n..
0020 33 31 e1 2b 00 50 f9 f6 39 a1 25 ca eb 8e 80 10  31.+P.. 9%....
0030 04 70 02 b3 00 00 01 01 08 0a 00 76 40 41 1e 63  .p..... ..v@A.c
    
```

Destination Hardware Address (eth.dst),... Packets: 1417 Displayed... Profile: Default

참고

- <http://kldp.org>
 - 한국 리눅스 문서 프로젝트
- <http://wiki.kldp.org/wiki.php/DocbookSgml/Libpcap-KLDP#COMPILE>
 - pcap_library 에 관련된 kldpwiki 사이트
- http://www.tcpdump.org/tcpdump_man.html
 - Tcpdump 매뉴얼
- <http://blog.naver.com/pjfile?Redirect=Log&logNo=40012816089>
 - Getopt() 함수에 관한 설명이 나와있는 곳 .
- <http://www.joinc.co.kr>
 - C 프로그래밍에 관한 참고자료가 풍부한 곳 .

끝

감사합니다 .