Data Communication assignment #1

데이터통신

컴퓨터학과

2015130741 원혜진

내용

1. Ethernet Packet Capture Using Wireshark 3

2. 802.11 Packet Capture Using Wireshark 4

3. PPP Execution 8

1. Ethernet Packet Capture Using Wireshark

1-1. Ping program의 Ethernet Header 분석 (Ethernet Environment)

1-1-0. Configurations

- IP configuration
  - 컴퓨터 IPv4 주소 : 211.243.74.115
  - 기본 게이트웨이 주소: 211.243.74.1
- Ethernet interface MAC address : 00-23-81-1B-75-1C
- WLAN MAC address : 80-19-34-5A-A2-DA

1-1-1. Request

: Request의 경우, 본인의 컴퓨터에서 기본 게이트웨이로 패킷을 전송하는 frame을 의미한다.

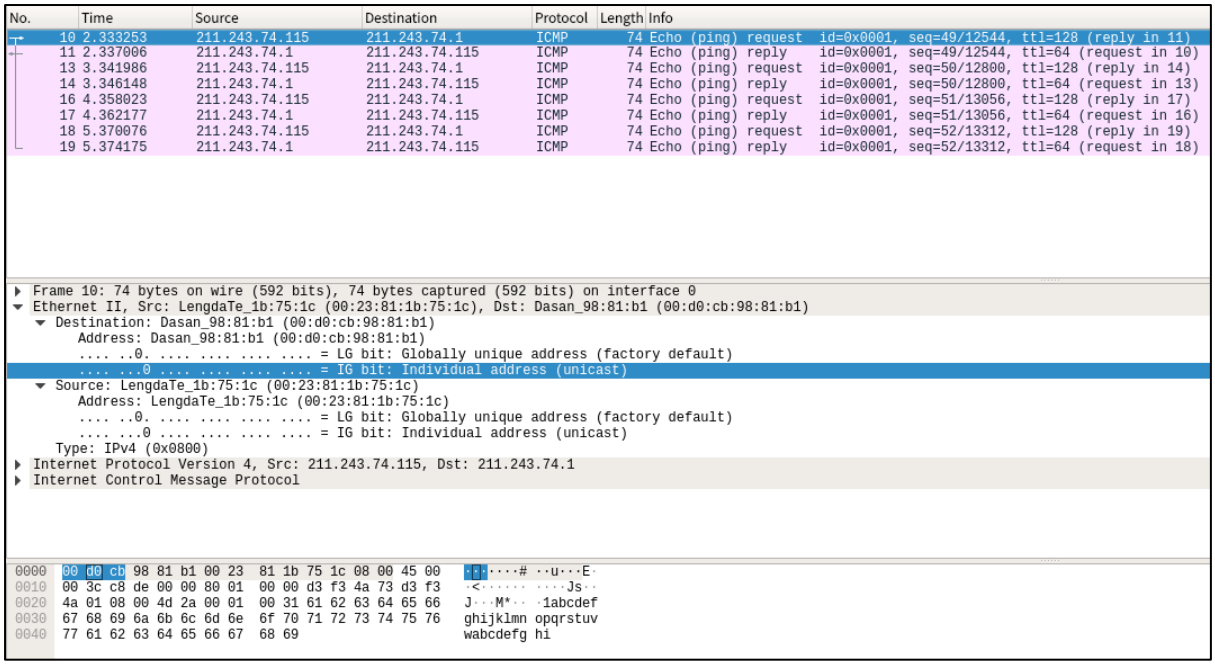
ethernet header 항목	wireshark	상세
DESTINATION ADDRESS	00:d0:cb:98:81:b1	기본 게이트웨이 MAC 주소
SOURCE ADDRESS	00:23:81:1b:75:1c	컴퓨터 MAC 주소
TYPE	0x0800	상위 레이어의 프로토콜을 의미한다. Network Layer에서 Ipv4를 사용하므로, 0x0800으로 표시되어 있다.

1-1-2. Reply

: Reply의 경우, 기본 게이트웨이에서 본인의 컴퓨터로 전송된 frame을 의미한다.

ethernet header 항목	wireshark	상세
DESTINATION ADDRESS	00:23:81:1b:75:1c	기본 게이트웨이에서 보내는 reply이므로, request와 source, destination이 반전되어 있다.
SOURCE ADDRESS	00:d0:cb:98:81:b1	
TYPE	0x0800	Request와 같은 이유로 Ipv4를 의미하는 0x0800으로 표시된다.

1-2. Wireshark capture



2. 802.11 Packet Capture Using Wireshark

2-1. Ping program의 IEEE 802.11 Header (IEEE 802.11 MAC, LLC, SNAP) 분석 (802.11 Environment)

2-1-0. Configurations : 1-1-0과 동일함

2-1-0 Request

Header 항목		Network Monitor	상세
MAC Header	FRAME CONTROL	0x0108	-00(bit0..1): Version -10(bit2..3): Type -0000(bit4..7): Subtype -1(bit8): To DS -0(bit9): From DS
	DURATION / ID	0x8000	
	ADDRESS 1	180F76 F9AE4B (BSSID, 수신)	WLAN interface(컴퓨터)는 데이터를 전송하기 전, AP에 연결되어야 하므로 AP WLAN interface의 MAC 주소가 필요하다. 때문에, 주소 값이 3개 필요하다.
	ADDRESS 2	801934 5AA2DA (SA, 발신)	
	ADDRESS 3	801934 5AA2DA (DA, 최종 수신)	

			컴퓨터 WLAN interface에서 발신->AP->컴퓨터 WLAN interface 순으로 패킷이 이동하므로, address1과 address3은 동일해야 한다.
	SEQUENCE CONTROL	0x0000	
	ADDRESS 4	-	
LLC	DSAP	0xAA	SNAP encapsulation을 사용하기 위해 0xAA로 표시한다.
	SSAP	0xAA	
	CONTROL	0x03	HDLC control 정의에 따른다. 해당 프레임은 ACK / 오류시 재전송 없이 user data를 주고받는 U-frame의 UI mode에 해당한다. U-frame이므로, bit1...0이 11로 표시된다.
SNAP	OUI	0x0000	SNAP는 Protocol Identifier로 사용되며, OUI는 0x0000가 default이다.
	Ethertype	0x0800	OUI가 0x0000이므로, 공식적인 protocol type값을 사용한다. (OUI가 non-zero일 경우, Ethertype은 OUI 부여한 기관이 정의) Network Layer에서 사용하는 프로토콜 : IPv4(0x0800)

2-1-0. Reply

Header 항목		Network Monitor	상세
MAC Header	FRAME CONTROL	0x4208	-00(bit0..1): Version -10(bit2..3): Type -0000(bit4..7): Subtype -0(bit8): To DS -1(bit9): From DS
	DURATION / ID	0x2C	
	ADDRESS 1	801934 5AA2DA (DA, 수신)	AP로부터 이동스테이션에 보내는 데이터프레임(

	ADDRESS 2	180F76 F9AE4B (BSSID, 발신)	To DS=0, From DS=1) Reply에 대해 ACK하는 주체는 컴퓨터 내 WLAN 인터페이스이므로, ADDRESS1에는 본인 컴퓨터의 WLAN MAC 주소가 표시된다.
	ADDRESS 3	180F76 F9AE4B (SA, 최초발신)	
	SEQUENCE CONTROL	0xF780	
	ADDRESS 4	-	
LLC	DSAP	0xAA	SNAP encapsulation을 사용하기 위해 0xAA로 표시한다.
	SSAP	0xAA	
	CONTROL	0x03	HDLC control 정의에 따른다. 해당 프레임은 ACK / 오류시 재전송 없이 user data를 주고받는 U-frame의 UI mode에 해당한다. U-frame이므로, bit1...0이 11로 표시된다.
SNAP	OUI	0x0000	SNAP는 Protocol Identifier로 사용되며, OUI는 0x0000가 default이다.
	Ethertype	0x0800	Network Layer에서 사용하는 프로토콜 : IPv4(0x0800)

2-1-0 Network Monitor와 Wireshark에서 header가 각각 다르게 표시되는 이유

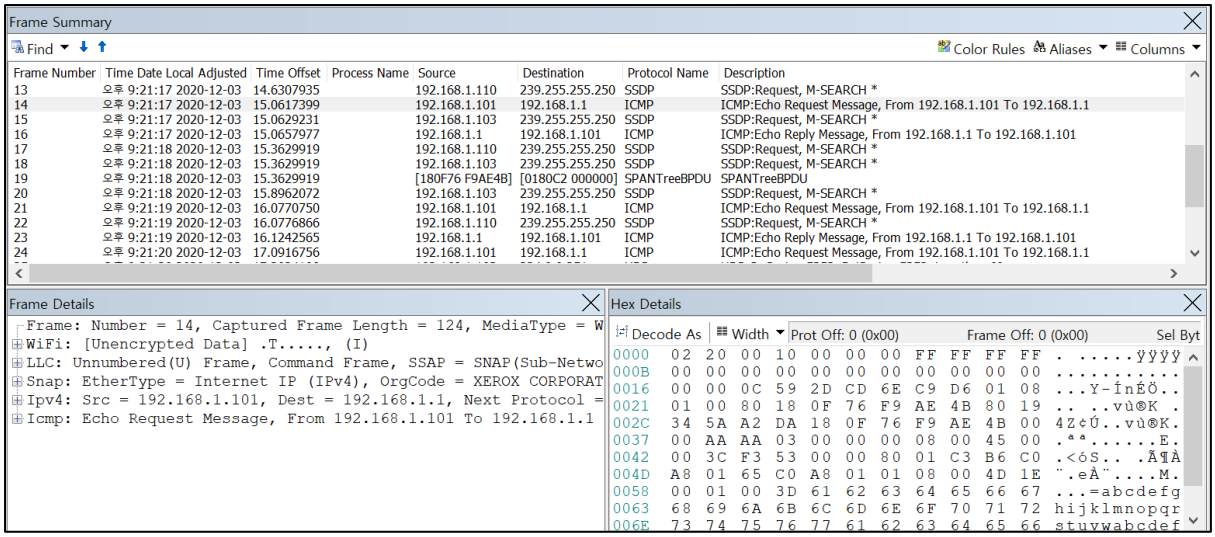
: 기본 설정 상에서는, WLAN의 패킷을 잡을 경우 802.11 management / control 패킷이 표시되지 않고, 802.11 패킷 헤더는 가짜 Ethernet header로 표시된다. [1]

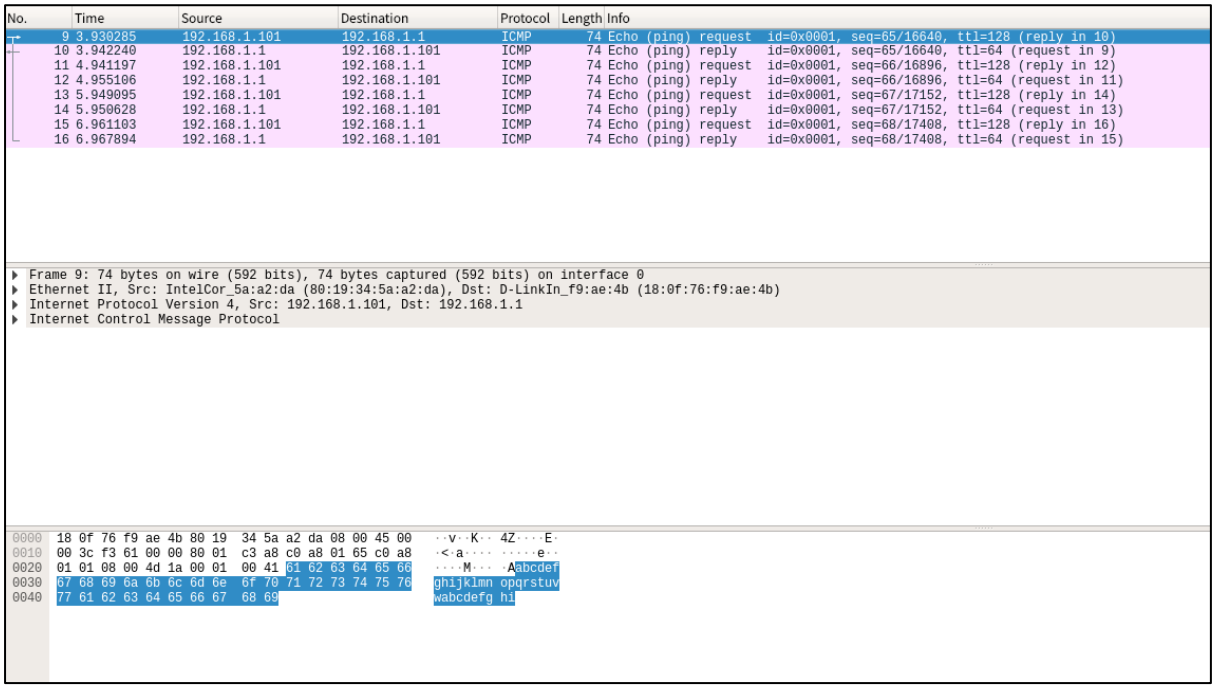
802.3에 비해, 802.11은 다루는 매체의 범위가 넓으므로(유선에 한정되지 않음) 이동하는 패킷의 수가 많다. 때문에, wireshark는 이를 정제하여 channel과 SSID를 기준으로 필터링한 패킷을 표시한다. 예시로 802.11 management / control패킷의 경우, Wireshark를 실행하는 기기에서(로) 발신(수신)되는 것 이외의 패킷에 해당하므로 표시되지 않는다.

WLAN 패킷을 정상적으로 캡쳐하기 위해서는 monitor mode로 설정 후 캡쳐해야 한다.

[1] https://wiki.wireshark.org/CaptureSetup/WLAN

2-2. network monitor, wireshark capture



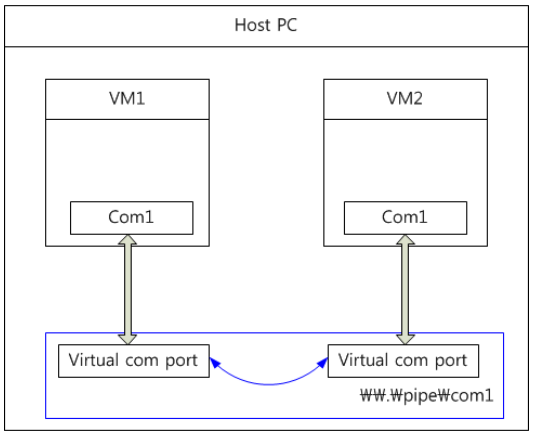


3. PPP Execution

3-1. Ping program의 Ethernet Header 분석 (Ethernet Environment)

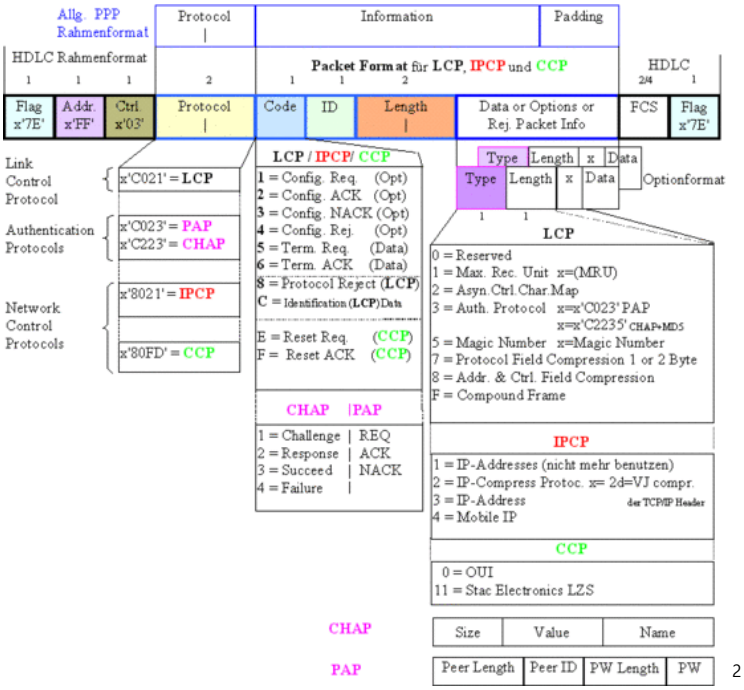
3-1-0. Configurations

-분석 환경



3-1-1. PPP

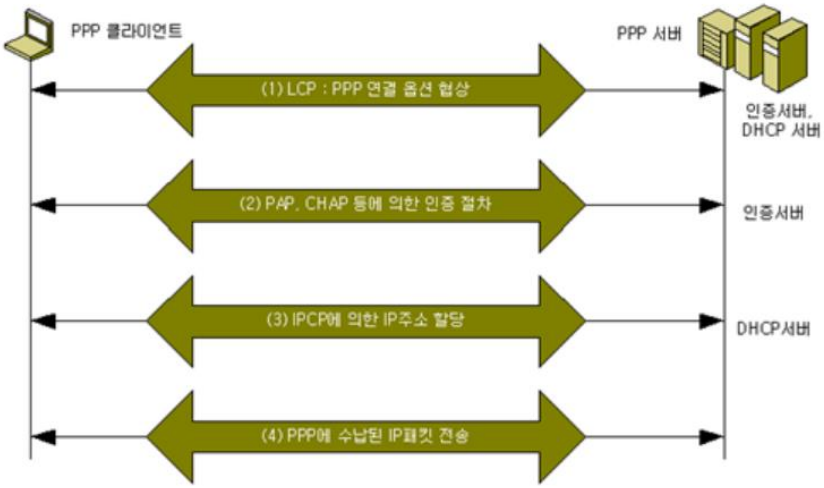
- PPP Frame의 format



[2]

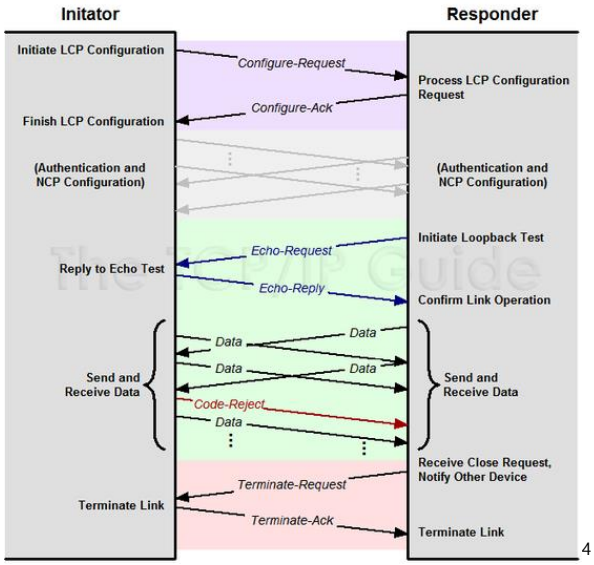
[2] https://m.blog.naver.com/PostView.nhn?blogId=sparc21&logNo=130189746467&proxyReferer=https:%2F%2Fwww.google.com%2F

- PPP의 Connection 과정



[3]

[PPP의 Connection 생성 과정]



[4]

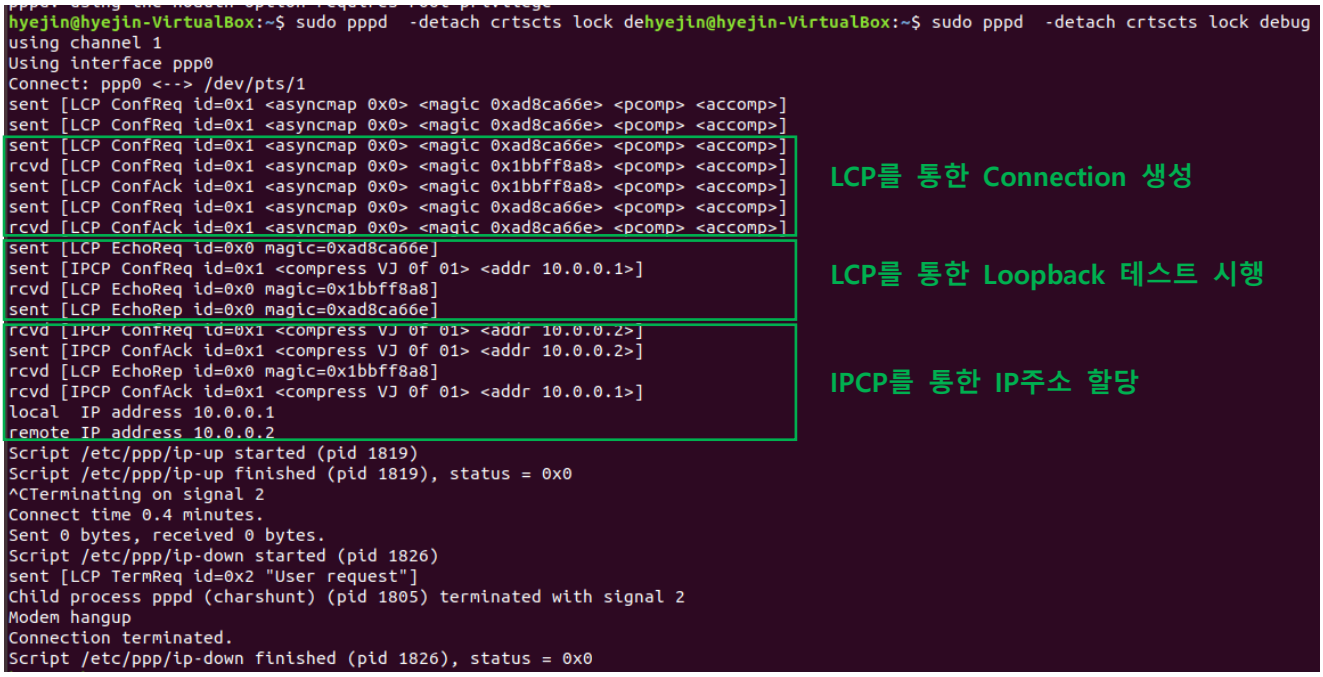
[LCP를 통한 링크 연결, 유지, 종료 과정]

[3] https://blog.naver.com/sol9501/70106935444

[4] https://m.blog.naver.com/PostView.nhn?blogId=sparc21&logNo=130189746467&proxyReferer=https:%2F%2Fwww.google.com%2F

3-1-2. pppd 분석

3-1-2-1. pppd debugging 분석



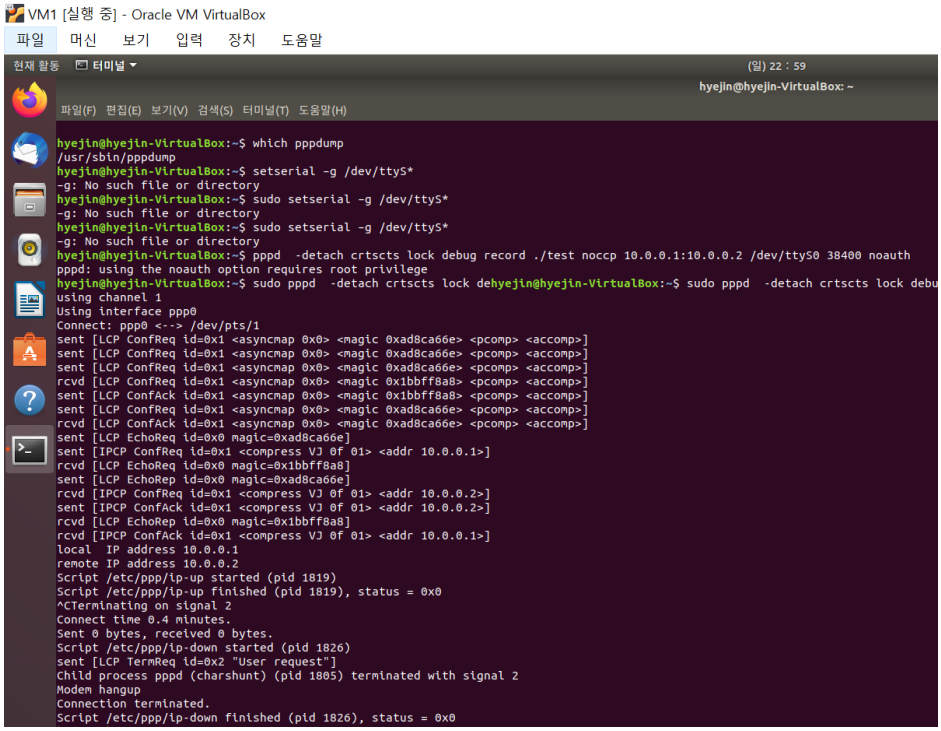
3-1-2-2. LCP Configure-Request 패킷 분석 (VM1 기준)

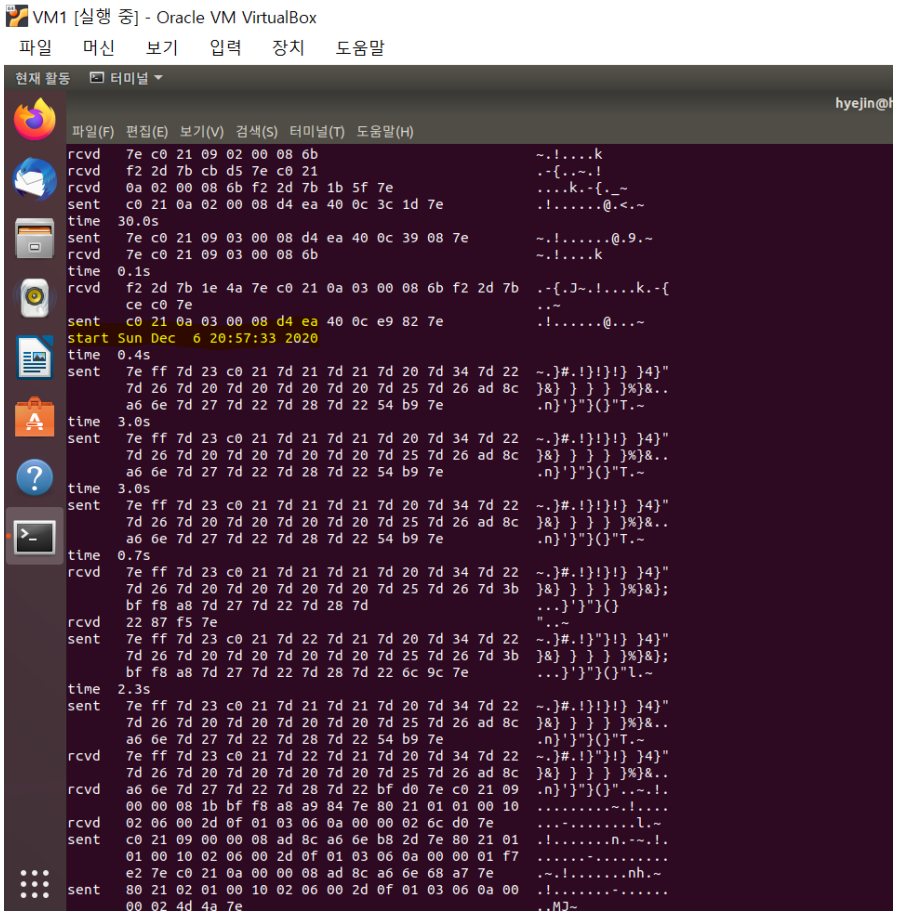
Header 항목 (괄호 내부는 presentation된 방식)					상세
Frame Delimeter	0x7e				
Address	0xff				all station address
Control	0x03(0x7d[5]23)				
HDLC Information	protocol	0xc021			Link Control Protocol
	PPP Information	Code	0x01(0x7d21)		Configure-Request
		ID	0x01(0x7d21)		request 와 reply 를 매칭하는 기준이 되는 field. 1 octet 으로 표시한다.
		Length	0x0018(0x7d20 7d34)		
		Option	Type	0x02(0x7d22)	Async-Control-Character-Map

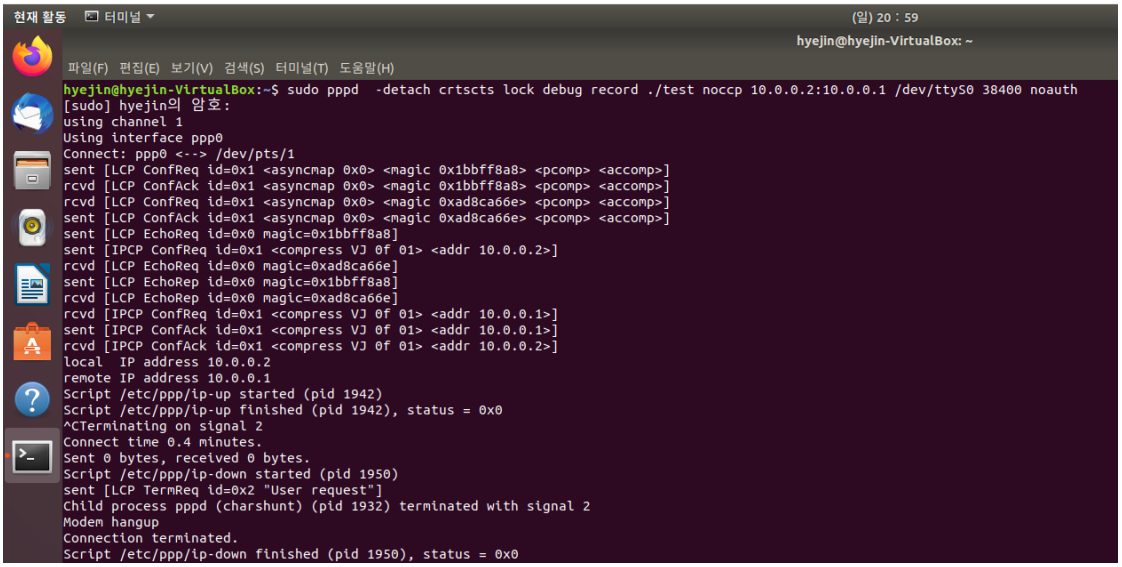
[5] 0x7d: Control Escape Octet. After FCS computation, the transmitter examines the entire frame between the two Flag Sequences. Each Flag Sequence, Control Escape octet, and any octet which is flagged in the sending Async-Control-Character-Map (ACCM), is replaced by a two octet sequence consisting of the Control Escape octet followed by the original octet exclusive-or'd with hexadecimal 0x20.

			Len	0x06(0x7d26)	LCP configuration option 의 길이는 1 octet 으로 표현되며, Type, Length, Data fields 를 포함한 길이를 의미한다.
			Data	0x0000 0000 (0x7d20 7d20 7d20 7d20)	
		Option	Type	0x05(0x7d25)	Magic-Number
			Len	0x06(0x7d 26)	
			Data	0x ad8c a66e	
		Option	Type	0x07(0x7d 27)	Protocol-Field-Compression
			Len	0x02(0x7d22)	
		Option	Type	0x08(0x7d28)	Address-and-Control-Field-Compression
			Len	0x02(0x7d22)	
CRC		0x54b9			
Frame Delimeter		0x7e			

3-2. pppd 실행화면


VM1 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
현재 활동 터미널
(일) 22 : 59
hyejin@hyejin-VirtualBox: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
hyejin@hyejin-VirtualBox:~$ which pppdump
/usr/sbin/pppdump
hyejin@hyejin-VirtualBox:~$ setserial -g /dev/ttyS*
-g: No such file or directory
hyejin@hyejin-VirtualBox:~$ sudo setserial -g /dev/ttyS*
-g: No such file or directory
hyejin@hyejin-VirtualBox:~$ sudo setserial -g /dev/ttyS*
-g: No such file or directory
hyejin@hyejin-VirtualBox:~$ pppd -detach crtscts lock debug record ./test noccp 10.0.0.1:10.0.0.2 /dev/ttyS0 38400 noauth
pppd: using the noauth option requires root privilege
hyejin@hyejin-VirtualBox:~$ sudo pppd -detach crtscts lock dehyejin@hyejin-VirtualBox:~$ sudo pppd -detach crtscts lock debu
using channel 1
Using interface ppp0
Connect: ppp0 <--> /dev/pts/1
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x1bbff8a8> <pcomp> <accomp>]
sent [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x1bbff8a8> <pcomp> <accomp>]
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
sent [LCP EchoReq id=0x0 magic=0xad8ca66e]
sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 10.0.0.1>]
rcvd [LCP EchoReq id=0x0 magic=0x1bbff8a8]
sent [LCP EchoRep id=0x0 magic=0xad8ca66e]
rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 10.0.0.2>]
sent [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 10.0.0.2>]
rcvd [LCP EchoRep id=0x0 magic=0x1bbff8a8]
rcvd [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 10.0.0.1>]
local IP address 10.0.0.1
remote IP address 10.0.0.2
Script /etc/ppp/ip-up started (pid 1819)
Script /etc/ppp/ip-up finished (pid 1819), status = 0x0
^CTerminating on signal 2
Connect time 0.4 minutes.
Sent 0 bytes, received 0 bytes.
Script /etc/ppp/ip-down started (pid 1826)
sent [LCP TermReq id=0x2 "User request"]
Child process pppd (charshunt) (pid 1805) terminated with signal 2
Modem hangup
Connection terminated.
Script /etc/ppp/ip-down finished (pid 1826), status = 0x0


VM1 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
현재 활동 터미널
hyejin@h
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
rcvd 7e c0 21 09 02 00 08 6b ~.!....k
rcvd f2 2d 7b cb d5 7e c0 21 .-{..~.!
rcvd 0a 02 00 08 6b f2 2d 7b 1b 5f 7e ....k.-{._~
sent c0 21 0a 02 00 08 d4 ea 40 0c 3c 1d 7e .!......@.<.~
time 30.0s
sent 7e c0 21 09 03 00 08 d4 ea 40 0c 39 08 7e ~.!......@.9.~
rcvd 7e c0 21 09 03 00 08 6b ~.!....k
time 0.1s
rcvd f2 2d 7b 1e 4a 7e c0 21 0a 03 00 08 6b f2 2d 7b .-{.J~.!....k.-{
ce c0 7e ..~
sent c0 21 0a 03 00 08 d4 ea 40 0c e9 82 7e .!......@...~
start Sun Dec 6 20:57:33 2020
time 0.4s
sent 7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22 ~.}#.!}!}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 ad 8c }&} } } } }%}&..
a6 6e 7d 27 7d 22 7d 28 7d 22 54 b9 7e .n}'}"}(}"T.~
time 3.0s
sent 7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22 ~.}#.!}!}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 ad 8c }&} } } } }%}&..
a6 6e 7d 27 7d 22 7d 28 7d 22 54 b9 7e .n}'}"}(}"T.~
time 3.0s
sent 7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22 ~.}#.!}!}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 ad 8c }&} } } } }%}&..
a6 6e 7d 27 7d 22 7d 28 7d 22 54 b9 7e .n}'}"}(}"T.~
time 0.7s
rcvd 7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22 ~.}#.!}!}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 3b }&} } } } }%}&};
bf f8 a8 7d 27 7d 22 7d 28 7d ...}'}"}(}
rcvd 22 87 f5 7e "..~
sent 7e ff 7d 23 c0 21 7d 22 7d 21 7d 20 7d 34 7d 22 ~.}#.!}"}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 3b }&} } } } }%}&};
bf f8 a8 7d 27 7d 22 7d 28 7d 22 6c 9c 7e ...}'}"}(}"l.~
time 2.3s
sent 7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22 ~.}#.!}!}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 ad 8c }&} } } } }%}&..
a6 6e 7d 27 7d 22 7d 28 7d 22 54 b9 7e .n}'}"}(}"T.~
rcvd 7e ff 7d 23 c0 21 7d 22 7d 21 7d 20 7d 34 7d 22 ~.}#.!}"}!} }4}"
7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 ad 8c }&} } } } }%}&..
rcvd a6 6e 7d 27 7d 22 7d 28 7d 22 bf d0 7e c0 21 09 .n}'}"}(}"..~.!.
00 00 08 1b bf f8 a8 a9 84 7e 80 21 01 01 00 10 ....~.!....
rcvd 02 06 00 2d 0f 01 03 06 0a 00 00 02 6c d0 7e ...-........l.~
sent c0 21 09 00 00 08 ad 8c a6 6e b8 2d 7e 80 21 01 .!.......n.-~.!.
01 00 10 02 06 00 2d 0f 01 03 06 0a 00 00 01 f7 ......-.........
e2 7e c0 21 0a 00 00 08 ad 8c a6 6e 68 a7 7e .~.!.......nh.~
sent 80 21 02 01 00 10 02 06 00 2d 0f 01 03 06 0a 00 .!.......-......
00 02 4d 4a 7e ..MJ~



```
hyejin@hyejin-VirtualBox:~$ sudo pppd  -detach crtscts lock debug record ./test noccp 10.0.0.2:10.0.0.1 /dev/ttyS0 38400 noauth
[sudo] hyejin의 암호:
using channel 1
Using interface ppp0
Connect: ppp0 <--> /dev/pts/1
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x1bbff8a8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x1bbff8a8> <pcomp> <accomp>]
rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
sent [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0xad8ca66e> <pcomp> <accomp>]
sent [LCP EchoReq id=0x0 magic=0x1bbff8a8]
sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 10.0.0.2>]
rcvd [LCP EchoReq id=0x0 magic=0xad8ca66e]
sent [LCP EchoRep id=0x0 magic=0x1bbff8a8]
rcvd [LCP EchoRep id=0x0 magic=0xad8ca66e]
rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 10.0.0.1>]
sent [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 10.0.0.1>]
rcvd [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 10.0.0.2>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
Script /etc/ppp/ip-up started (pid 1942)
Script /etc/ppp/ip-up finished (pid 1942), status = 0x0
^CTerminating on signal 2
Connect time 0.4 minutes.
Sent 0 bytes, received 0 bytes.
Script /etc/ppp/ip-down started (pid 1950)
sent [LCP TermReq id=0x2 "User request"]
Child process pppd (charshunt) (pid 1932) terminated with signal 2
Modem hangup
Connection terminated.
Script /etc/ppp/ip-down finished (pid 1950), status = 0x0
```

```
hyejin@hyejin-VirtualBox:~$ pppdump -h ./test
start Sat Dec  5 16:56:48 2020
time  0.5s
rcvd   7d 21 7d 20 7d 34 7d 22 7d 26 7d 20 7d 20 7d 20  }!} }4}"}&} } }
       7d 20 7d 25 7d 26 c2 a2 8a b1 7d 27 7d 22 7d 28  } }%}&....}'}"}(
       7d 22 7d 3a 7d 3f 7e                             }":}:}?~
time  0.1s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
time  3.0s
sent   7e ff 7d 23 c0 21 7d 21 7d 21 7d 20 7d 34 7d 22  ~.}#.!}!}!} }4}"
       7d 26 7d 20 7d 20 7d 20 7d 20 7d 25 7d 26 7d 21  }&} } } } }%}&}!
       e0 58 34 7d 27 7d 22 7d 28 7d 22 f0 2a 7e        .X4}'}"}(}".*~
```