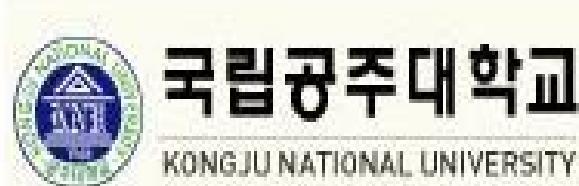


[R E P O R T]

정보통신공학전공
200301582
김성태



과제 8: 가상 네트워크에서 E-Mail 서버 구축

1. 개요

4 계층으로 구성되는 가상 네트워크에서 E-Mail 서버를 구축하고 동작을 확인한다.

2. 수행할 과제 내용

메일 서버 구축

필요한 수만큼의 메일 서버를 구축한 후 동작을 확인한다.

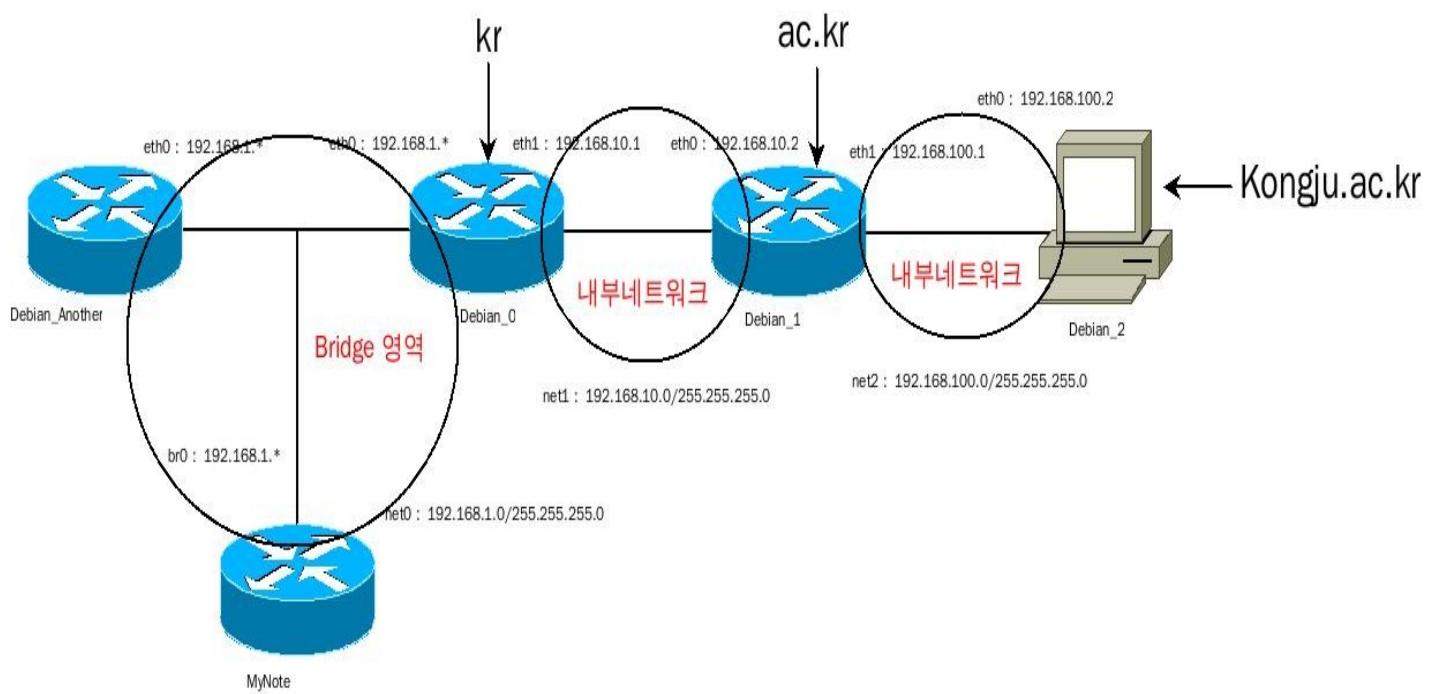
클라이언트에서 nslookup 으로 3 명의 수신측 도메인의 메일서버를 확인하고, 확인한 화면을 캡쳐하여 보고서에 추가한다.

XP 내 Outlook 을 사용하여 메일을 보내고 받아본다.

메일이 전달될 때 수반되는 트래픽을 sms tm 으로 잡아서 메일 전달 관련 세부 동작 절차를 분석한다.

전달된 3개의 메일(반드시 송신자, 수신자 도메인명이 보이도록 할 것)과 기타 중요한 부분을 캡쳐하여 보고서에 추가하고, 아울러 동작절차 분석 내용 및 결과도 보고서에 추가한다.

3. 네트워크의 구성



4. 메일 서버 동작방식(E-mail 전달 과정)

E-mail 은 Mail_ID@Domain_Name 과 같은 주소의 형태에서 알 수 있듯이 도메인 네임을 기본적인 배경으로 하고 있다. 그러므로 전송된 E-mail 이 최종 수신자를 찾는 과정은 네임서버의 질의 과정과 동일한 과정을 거친다. 하지만 그것은 최종 수신자에 해당되는 도메인 네임을 찾는 과정일 뿐이고, E-mail 이 송수신되는 과정은 이보다 좀 복잡하다.

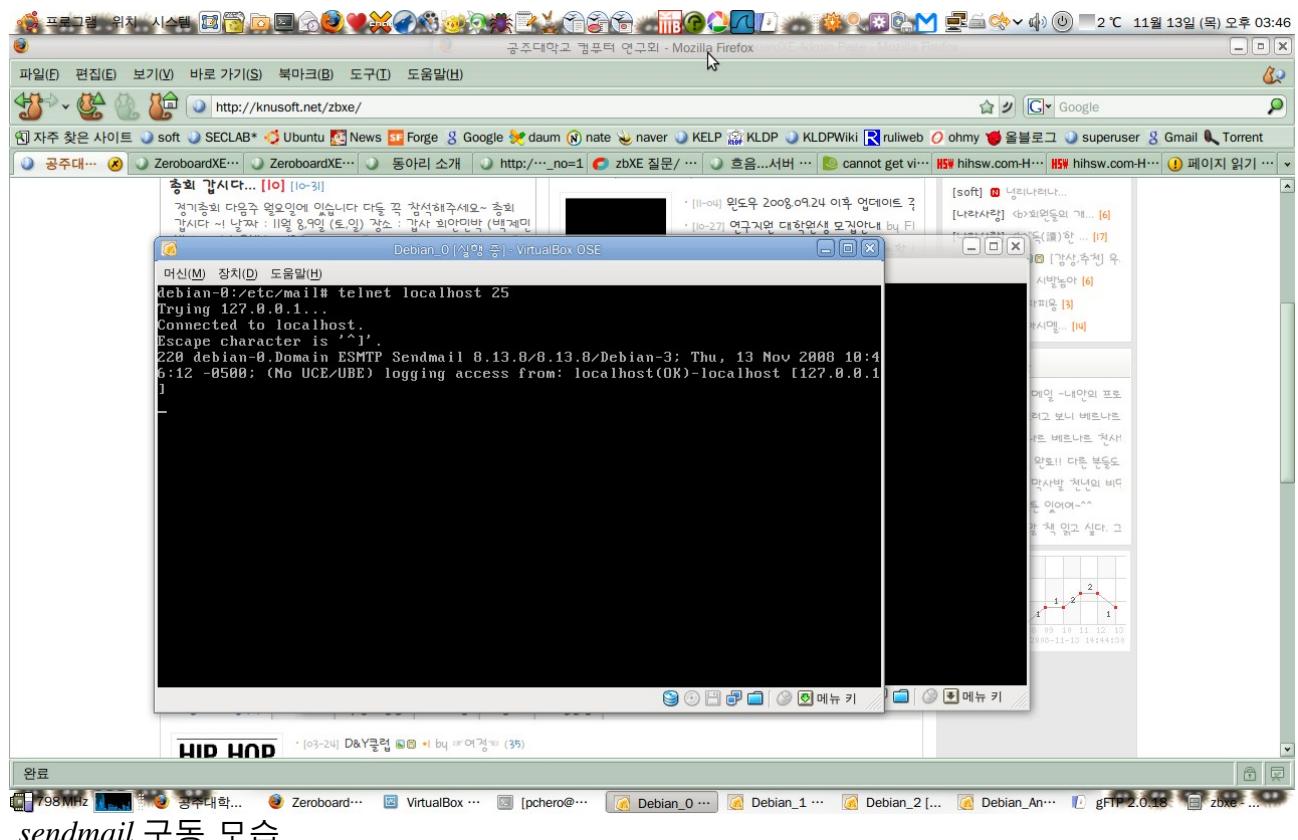
이를 순서로 나타내면 다음과 같다.

1. 사용자가 MUA(Outlook Express 등)를 사용하여 E-mail을 전송한다.
2. 사용자가 가입한 ISP 업체의 인터넷 회선을 따라서 ISP 업체에서 서비스하는 보내는 메일서버(SMTP 서버)에 E-mail이 저장(MTA) 된다.
3. SMTP 서버는 로컬 네임서버에 질의하여 수신할 E-mail의 도메인 네임을 관리하는 네임서버를 찾는다. 만약 네임서버를 찾지 못했으면 E-mail은 송신한 MUA로 다시 회송시킨다.
4. 네임서버를 찾았으면 그 네임서버에 질의하여 해당되는 도메인 네임의 메일 익스체인저(MX)와 연결된 받는 메일서버(MTA)를 찾는다. MTA는 대부분 POP3를 사용한다.
5. 받는 메일서버(MTA)의 주소를 확인하였으면 SMTP 서버는 MTA에 저장된 E-mail을 POP3 서버로 전송시킨다. 만약 E-mail의 도메인 네임은 맞지만 메일서버의 사용자 계정이 없는 것이거나 접속을 거부하는 호스트라면 POP3 서버는 E-mail 수신을 거부한다. E-mail 수신이 거부되면 SMTP 서버는 바로 송신한 MUA로 회송한다.
6. POP3 서버는 E-mail을 저장하고 최종 수신자가 MUA를 사용하여 새로운 E-mail을 확인할 때 까지 가지고 있는데
7. 최종 수신자가 MUA를 가동시키면 POP3 서버는 사용자 인증을 거친 다음 E-mail을 전송해 주고 저장된 내용을 삭제한다.

위와 같은 과정을 간단히 묘사하면 MUA -> 보내는 메일서버 -> 받는 메일서버 -> MUA가 된다.

5. 실험 결과

메일 서버 구축



파일(F) 편집(E) 보기(V) 터미널(I) 탭(I) 도움말(H)

pchero@MyNote: ~ soft@toy2: ~/public_html pchero@MyNote: ~

```
pchero@MyNote:~$ telnet 192.168.1.8 25
Trying 192.168.1.8...
Connected to 192.168.1.8.
Escape character is '^'.
220 debian-0.Domain ESMTP Sendmail 8.13.8/8.13.8/Debian-3; Thu, 13 Nov 2008 11:5
5:27 -0500: (No UCE/UBE) logging access from: [192.168.1.104](FAIL)-[192.168.1.1
04]
```

텔넷을 이용한 원격 메일 서버 접속

프로그램 위치 시스템

Debian_0 [설정 중] VirtualBox OSE

파일(F) 편집(E) 보기(V) 바로 가기(S) 북마크(B)

자주 찾은 사이트 soft SECLAB* Ubuntu

KLDWiki: SSL-POP3S_SMT... 엘파스 가

```
머신(M) 장치(D) 도움말(H)
debian-0:/etc/xinetd.d# telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^}'.
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS LOGINDISABLED] localhost IMAP4rev1 2803.339 at Thu, 13 Nov 2008 12:49:36 -0500 (EST)
^]
telnet> exit
?Invalid command
telnet> quit
Connection closed.
debian-0:/etc/xinetd.d# _
```

3.2. pop3s 서비스 시작

- # vi /etc/xinetd.d/pop3s

```
service pop3s
{
    disable
    socket_type
    wait
    user
    server
    log_on_sucess
    log_on_failure
}
```

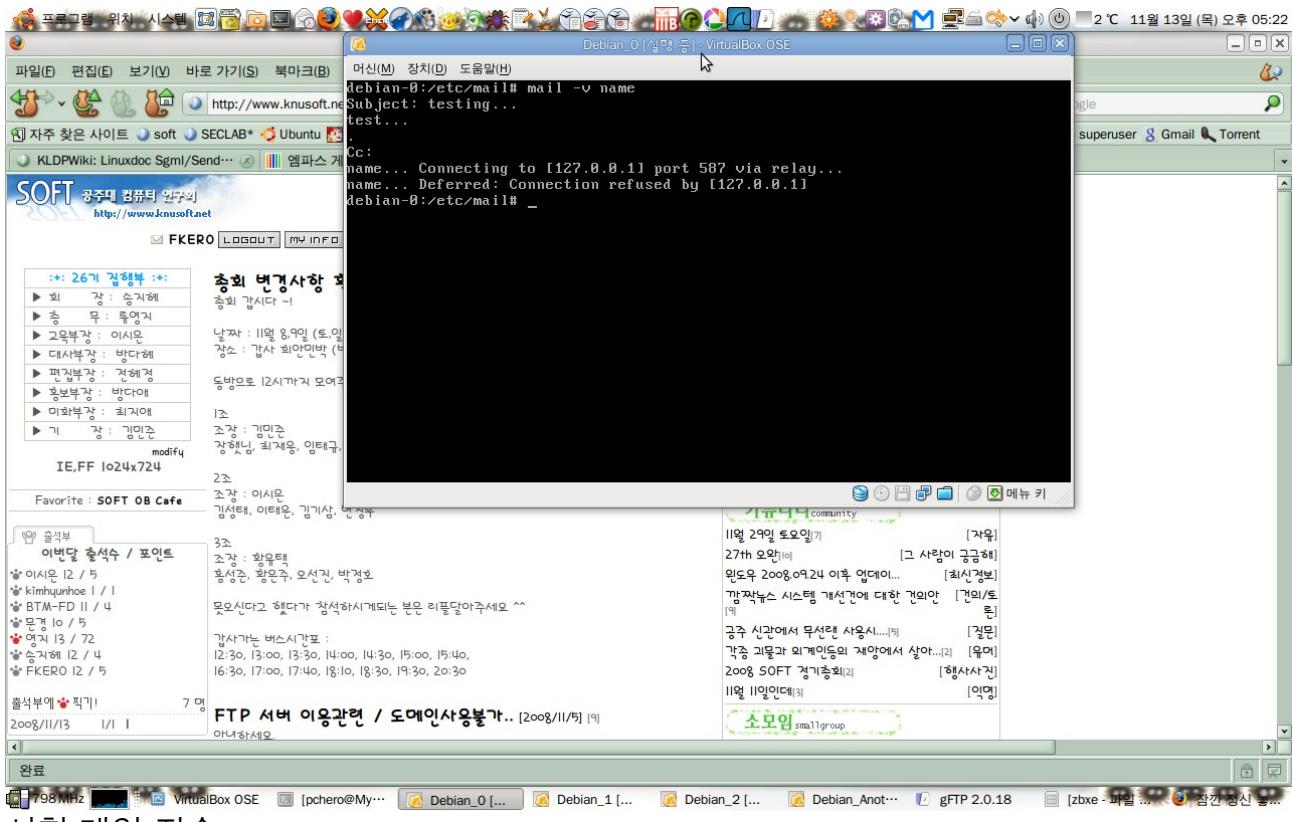
/etc/init.d/xinetd restart

3.3. sendmail 설정하고 재시작하기.

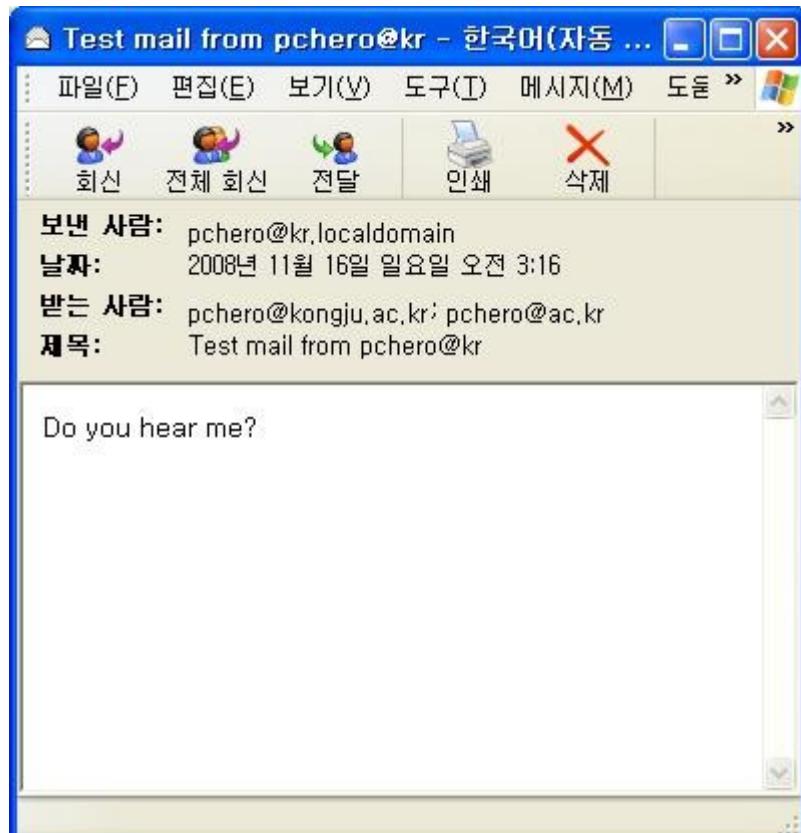
- # vi /etc/mail/sendmail.mc, 다음 내용을 추가한다.

```
define(`confCACERT_PATH', `/usr/share/ssl/certs')dnl
define(`confCACERT', `/usr/share/ssl/certs/cacert.crt')dnl
define(`confSERVER_CERT', `/usr/share/ssl/certs/sendmail.pem')dnl
define(`confSERVER_KEY', `/usr/share/ssl/certs/cert.key')dnl
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
CwInvaNgnd.com
```

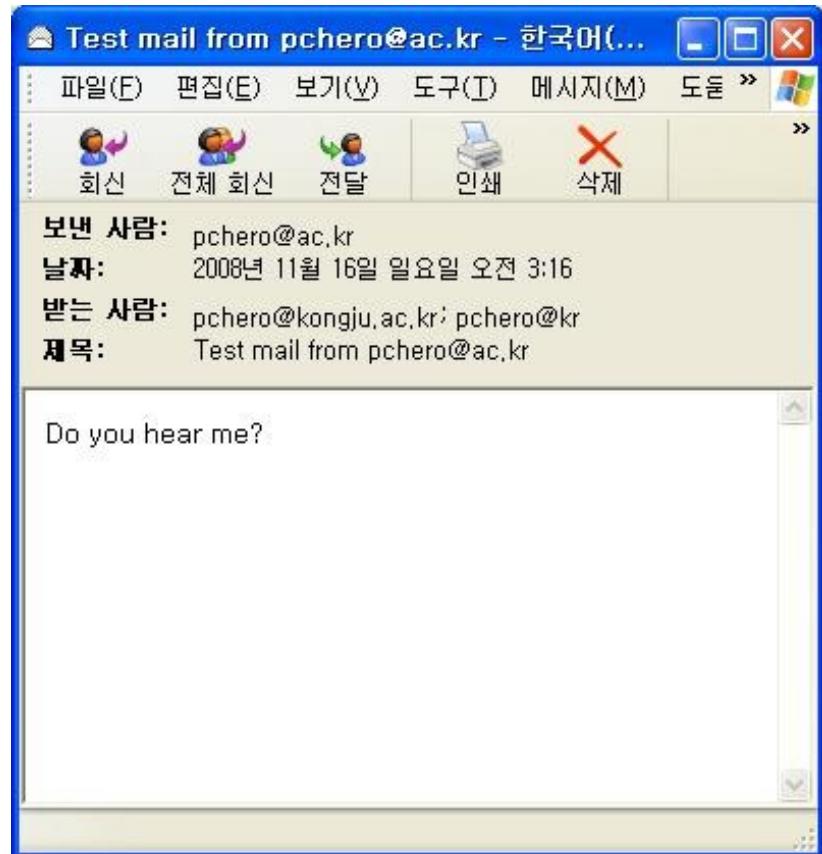
텔넷을 이용한 원격 POP3 서버 접속



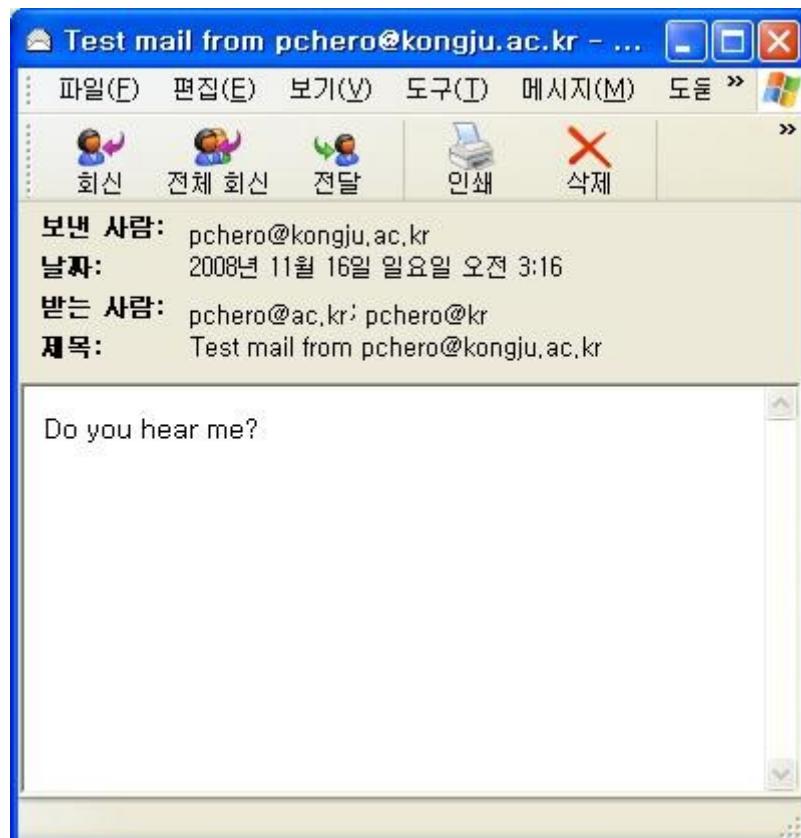
시험 메일 전송



pchero@kr에서 발송한 메일



pchero@ac.kr에서 보낸 사진



pchero@kongju.ac.kr에서 보낸 메시지

NVIDIA nForce MCP Networking Adapter Driver (Microsoft's Packet Scheduler) : Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.10.2	TCP	config-port > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460
2	0.000489	192.168.10.2	192.168.1.2	TCP	smtp > config-port [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.000516	192.168.1.2	192.168.10.2	TCP	config-port > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.025137	192.168.10.2	192.168.1.2	TCP	32807 > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=1063597 TSER=0 WS=0
5	3.015414	192.168.10.2	192.168.1.2	TCP	32807 > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=1063897 TSER=0 WS=0
6	5.019184	192.168.10.2	192.168.1.2	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.11.2/8.11.2; Sun, 16 Nov 2008 C
7	5.020233	192.168.1.2	192.168.10.2	SMTP	Command: HELO SOFT4
8	5.020891	192.168.10.2	192.168.1.2	SMTP	smtp > config-port [ACK] Seq=90 Ack=13 Win=5840 Len=0
9	5.021000	192.168.10.2	192.168.1.2	SMTP	Response: 250 localhost.localdomain Hello [192.168.1.2], pleased to meet you
10	5.021864	192.168.1.2	192.168.10.2	SMTP	Command: MAIL FROM: <pchero@ac.kr>
11	5.026819	192.168.10.2	192.168.1.2	SMTP	Response: 250 2.1.0 <pchero@ac.kr>... Sender ok
12	5.027118	192.168.1.2	192.168.10.2	SMTP	Command: RCPT TO: <pchero@kongju.ac.kr>
13	5.030691	192.168.10.2	192.168.1.2	SMTP	Response: 250 2.1.5 <pchero@kongju.ac.kr>... Recipient ok
14	5.030977	192.168.1.2	192.168.10.2	SMTP	Command: DATA
15	5.031451	192.168.10.2	192.168.1.2	SMTP	Response: 354 Enter mail, end with "." on a line by itself
16	5.032039	192.168.1.2	192.168.10.2	SMTP	DATA fragment, 1230 bytes
17	5.066130	192.168.10.2	192.168.1.2	TCP	smtp > config-port [ACK] Seq=296 Ack=1308 Win=7380 Len=0
18	5.066176	192.168.1.2	192.168.10.2	IMF	from: <pchero@ac.kr>, subject: tes, (text/plain) (text/html)
19	5.066493	192.168.10.2	192.168.1.2	TCP	smtp > config-port [ACK] Seq=296 Ack=1313 Win=7380 Len=0
20	5.073116	192.168.10.2	192.168.1.2	SMTP	Response: 250 2.0.0 mag8q5r02536 Message accepted for delivery
21	5.073471	192.168.1.2	192.168.10.2	SMTP	Command: QUIT
22	5.075051	192.168.10.2	192.168.1.2	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
23	5.075248	192.168.1.2	192.168.10.2	TCP	config-port > smtp [FIN, ACK] Seq=1319 Ack=402 Win=65134 Len=0
24	5.079851	192.168.10.2	192.168.1.2	TCP	smtp > config-port [FIN, ACK] Seq=402 Ack=1320 Win=7380 Len=0

Frame 14 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: Asiarock_95:db:94 (00:19:66:95:db:94), Dst: VMware_00:92:d4 (00:0c:29:00:92:d4)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.10.2 (192.168.10.2)

Transmission Control Protocol, Src Port: config-port (3577), Dst Port: smtp (25), Seq: 72, Ack: 246, Len: 6

Source port: config-port (3577)
 Destination port: smtp (25)
 Sequence number: 72 (relative sequence number)
 [Next sequence number: 78 (relative sequence number)]
 Acknowledgement number: 246 (relative ack number)
 Header length: 20 bytes
 Flags: 0x18 (PSH, ACK)
 Window size: 65290
 Checksum: 0xa495 [correct]
 [SEQ/ACK analysis]

Simple Mail Transfer Protocol
 Command: DATA\r\n Command: DATA

Frame (frame), 60 bytes

Packets: 31 Displayed: 31 Marked: 0

Profile: Default

0000 00 0c 29 00 92 d4 00 19 66 95 db 94 08 00 45 00 .). F....E.
 0010 00 2e be d7 40 00 80 06 af 9d c0 a8 01 02 c0 a8 ..:@.O....P.
 0020 0a 02 0d f9 00 19 ab 89 e5 30 b6 ec 84 8b 50 18DA TA..
 0030 ff 0a a4 95 00 00 44 41 54 41 0d 0a

SMTP 패킷을 Wireshark 을 이용하여 캡쳐한 모습