

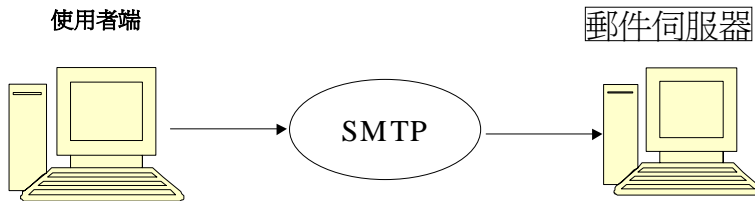


第 29 章
郵件伺服器
Sendmail

第 29 章 郵件伺服器 Sendmail

E-mail 傳送分為 SMTP(Simple Mail Transport Protocol)簡單寄信協定與 POP(Post Office Protocol)收信協定.我們只要在我們的 E-mail 設定此兩項就可以收發信了,當然在外面也要向 ISP 公司申請電子郵件帳號與密碼。我們使用者透過 SMTP 協定將郵件寄送到遠端的郵件伺服器,再由遠端的郵件伺服器經過 POP3 協定來發送郵件到使用者端。

寄信過程

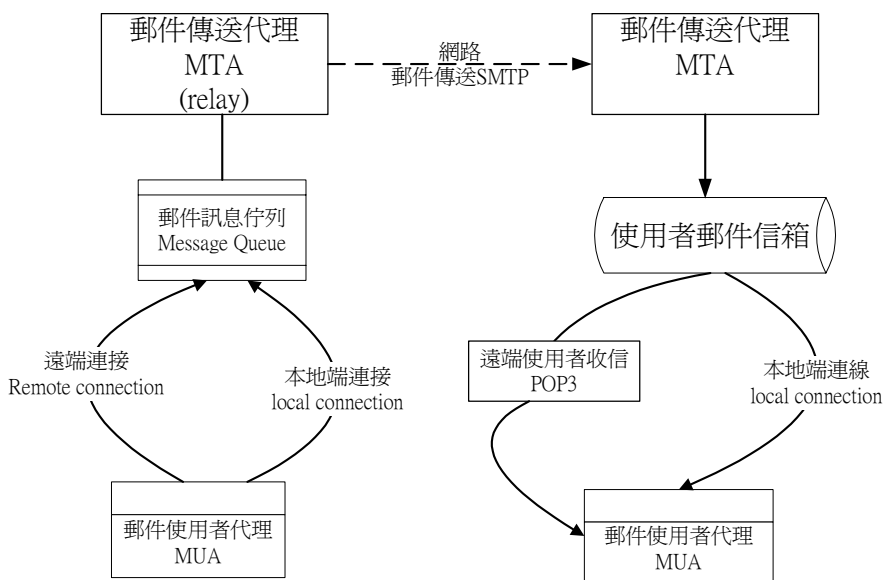


收信過程



這裏顯示從一個人寄 e-mail 訊息給另外一個人的電子郵件郵寄過程。不管這個使用者是在遠端或 local 本地端收發電子郵件，這個路徑就會像下圖一樣。當使用者使用 Outlook 來發送已經寫好的電子郵件(這邊稱為 Mail User Agent 郵件使用者代理 MUA)，這個 message 訊息會傳送到 SMTP 伺服器的郵件訊息佇列 Message Queue(這邊稱為 Mail Transfer Agent 郵件傳輸代理 MTA)。當郵件傳送代理一收到這個電子郵件，就會立刻轉信(relay)到相關的郵件傳送代理 MTA，並且放到該地址的使用者郵件信箱。在這遠端的郵件傳輸代理 MTA，它放置這郵件到使用者的郵件信箱，它可以被本地端連線的使用者讀取，也可以被遠端的使用者透過 POP3 的協定來收信。

我們當 RedHat Linux Fadora 1 的管理者要知道郵件伺服器 Sendmail 的操作方式就是 MTA 郵件傳輸代理，也要知道傳送、轉信和接收的角色，我們也要知道郵件使用者代理程式 MUA，其接收和上傳郵件的方法，而訊息佇列 Message Queue 和使用者的郵件信箱就是暫時存放電子郵件的地方。



電子郵件郵寄過程



Mail Transfer Agent (郵件傳輸代理 MTA)和 Mail User Agent(郵件使用者代理 MUA)

	MTA(郵件傳輸代理 MTA)	MUA(郵件使用者代理 MUA)
微軟的產品	Microsoft Exchange 郵件伺服器	Microsoft Outlook/Outlook Express 使用者端電子郵件收發程式。
Unix 的產品	Sendmail 郵件伺服器、Postfix 郵件伺服器	Pine、Elm、Mutt 和 Netscape Mail 等使用者端電子郵件收發程式。

29-1 郵件伺服器(sendmail)設定

我們可以使用 `ps -x|more` 指令來看，目前有哪些行程在跑，我們的 sendmail 已經啟動了，pid 是行程的優先編號(ID)。在下圖中 Sendmail 的 pid 是 1138。

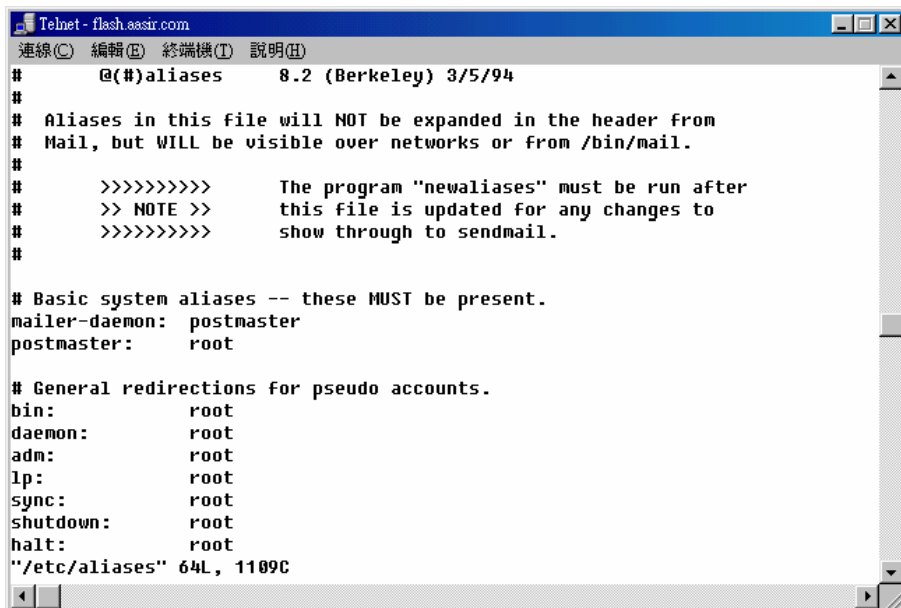
```

Telnet - flash.aasir.com
連線(C) 編輯(E) 終端機(T) 說明(H)
1028 ?      S      0:00 rpc.mountd
1034 ?      SW     0:00 [nfsd]
1035 ?      SW     0:00 [lockd]
1036 ?      SW     0:00 [rpciod]
1037 ?      SW     0:00 [nfsd]
1038 ?      SW     0:00 [nfsd]
1039 ?      SW     0:00 [nfsd]
1040 ?      SW     0:00 [nfsd]
1041 ?      SW     0:00 [nfsd]
1042 ?      SW     0:00 [nfsd]
1043 ?      SW     0:00 [nfsd]
1082 ?      S      0:00 /bin/sh /usr/bin/safe_mysqlld --defaults-file=/etc/r
1138 ?      S      0:00 sendmail: accepting connections
1166 ?      SW     0:00 [scsi_eh_0]
1185 ?      S      0:00 gpm -t ps/2 -m /dev/mouse
1226 ?      S      0:00 crond
1260 ?      S      0:00 squid -D
1463 tty1   S      0:00 /sbin/mingetty tty1
1464 tty2   S      0:00 /sbin/mingetty tty2
1465 tty3   S      0:00 /sbin/mingetty tty3
1466 tty4   S      0:00 /sbin/mingetty tty4
1467 tty5   S      0:00 /sbin/mingetty tty5
--More--

```

我們可以編輯 sendmail 的別名設定，每一個使用者都可以設定多個別名，在 /etc/aliases 的檔案中，bin、daemon、adm、lp 和 sync 都對應到 root 使用者，因此 root 使用者有這麼多別名。

```
#vi /etc/aliases
```



```
Telnet - flash.aasir.com
# @(#)aliases      8.2 (Berkeley) 3/5/94
#
# Aliases in this file will NOT be expanded in the header from
# Mail, but WILL be visible over networks or from /bin/mail.
#
# >>>>>>>>      The program "newaliases" must be run after
# >> NOTE >>      this file is updated for any changes to
# >>>>>>>>      show through to sendmail.
#
# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster:    root

# General redirections for pseudo accounts.
bin:           root
daemon:       root
adm:          root
lp:           root
sync:         root
shutdown:     root
halt:         root
"/etc/aliases" 64L, 1109C
```

<<1>>啟動 sendmail



```
Telnet - flash.aasir.com
[root@flash home]# /etc/rc.d/init.d/sendmail restart
Shutting down sendmail: [ OK ]
Starting sendmail: [ OK ]
[root@flash home]#
```



<<2>>檢查郵件的佇列

我們使用 mailq 來檢查目前尚未處理的信件。

```
[root@flash home]# mailq
/var/spool/mqueue is empty
```

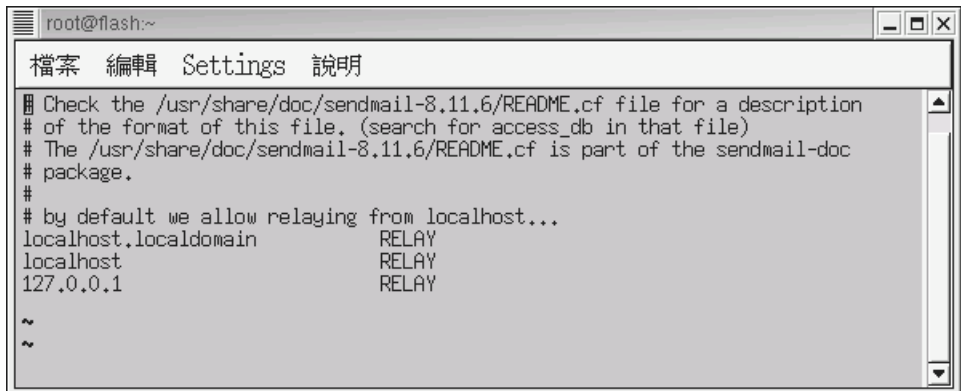
<<3>>限制或收發某一些網域或使用者的郵件

我們可以限制或收發某一些網域或使用者的信，使用/etc/mail/access 這個檔案。



```
root@flash:~
檔案 編輯 Settings 說明
[root@flash root]# vi /etc/mail/access
```

在第一個參數是指定某個網域或 IP，而第二個參數是指定允許郵件是否接收或寄送。



```
root@flash:~
檔案 編輯 Settings 說明
# Check the /usr/share/doc/sendmail-8.11.6/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail-8.11.6/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain    RELAY
localhost                 RELAY
127.0.0.1                 RELAY
~
~
```

當第二個參數是 OK 則允許接收及寄送指定網址的信件。

當第二個參數是 RELAY 時，則允許中繼網址要求轉寄的郵件。

當第二個參數是 REJECT 時，則拒絕接收或寄送指定網址的信件。

當第二個參數是 DISCARD，則丟棄所寄過來的郵件。

/etc/mail/access 這存取資料庫提供一個方法來應用特定的規則到主機、子網域或位置群組。這些應用的規則包括 OK、REJECT、RELAY 和 DISCARD。

/etc/mail/access 的存取選項	說明
OK	OK 則允許接收及寄送指定網址的信件。
REJECT	REJECT 時，則拒絕接收或寄送指定網址的信件。
DISCARD	DISCARD，則丟棄所寄過來的郵件。
RELAY	RELAY 時，則允許中繼網址要求轉寄的郵件。
550<message>	指定拒絕訊息給指定的傳送者主機。

我們可以限制或收發某一些網域或使用者的信，使用/etc/mail/access 這個檔案。

```
#vi /etc/mail/access
```

在第一個參數是指定某個網域或 IP，而第二個參數是指定允許郵件是否接收或寄送。

第一行的 550 是拒絕從 cyberspammer.com 來接收郵件，並且會顯示訊息，最後一行是允許從 128.32 的子網域來轉信。

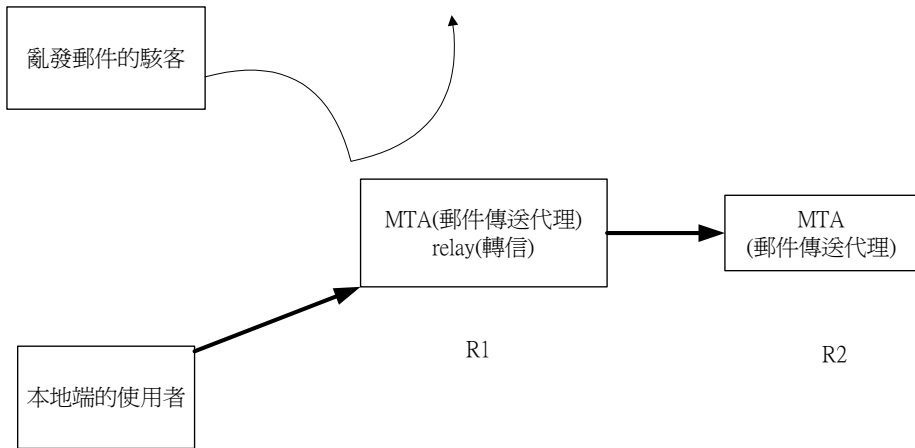
```
cyberspammer.com    550 We don't accept mail from spammers
FREE.STEALTH.MAILER@ 550 We don't accept mail from spammers
another.source.of.spam          REJECT
okay.cyberspammer.com          OK
128.32                        RELAY
```

當我們修改/etc/mail/access 後，這 access.db 檔一定要被重新產生。我們可以使用 makemaps 指令來重新更新 access.db 的檔案，然後再重新啟動郵件伺服器的主行程。



```
# /usr/sbin/makemap hash access.db < access
```

在 Sendmail 郵件伺服器中，預設是只有本地端(local)合法的使用者才能夠使用郵件代理 MTA 來轉信。當我們要由 R1 的地方郵寄信件到 R2 的地方時，只有在本地端的使用者才能夠使用郵件傳送代理來轉信到 R2 的地方。在中限制非本地端的使用者(遠端亂發郵件的駭客)使用 MTA 郵件傳送代理來轉信，駭客的信會被我們丟掉。



<<4>>設定郵件伺服器的組態

我們可以使用 `vi /etc/mail/sendmail.cf` 來設定郵件伺服器的組態。

```
[root@flash chaiyen]# vi /etc/mail/sendmail.cf
```




```
root@flash:~  
檔案 編輯 Settings 說明  
1 #  
2 # Copyright (c) 1998-2001 Sendmail, Inc. and its suppliers.  
3 # All rights reserved.  
4 # Copyright (c) 1983, 1995 Eric P. Allman. All rights reserved.  
5 # Copyright (c) 1988, 1993  
6 # The Regents of the University of California. All rights reserved.  
7 #  
8 # By using this file, you agree to the terms and conditions set  
9 # forth in the LICENSE file which can be found at the top level of  
10 # the sendmail distribution.  
11 #  
12 #  
13  
14 #####  
15 #####  
16 #####  
17 ##### SENDMAIL CONFIGURATION FILE  
18 #####  
19 #####  
20 #####  
21 #####  
22  
23 ##### $Id: cfhead.m4,v 8.76.4.16 2001/03/06 22:56:36 ca Exp $ #####  
24 ##### $Id: cf.m4,v 8.32 1999/02/07 07:26:14 gshapiro Exp $ #####  
25  
26 ##### linux setup for Red Hat Linux #####  
27 ##### $Id: linux.m4,v 8.11.16.2 2000/09/17 17:04:22 gshapiro Exp $ #####  
28  
29  
30
```

```
root@flash:~  
檔案 編輯 Settings 說明  
32  
33  
34  
35 ##### $Id: no_default_msa.m4,v 8.1.10.1 2000/09/17 17:04:22 gshapiro Exp $ #####  
36  
37 ##### $Id: smrsh.m4,v 8.14 1999/11/18 05:06:23 ca Exp $ #####  
38  
39 ##### $Id: mailertable.m4,v 8.18 1999/07/22 17:55:35 gshapiro Exp $ #####  
40  
41 ##### $Id: virtusertable.m4,v 8.16 1999/07/22 17:55:36 gshapiro Exp $ #####  
42  
43 ##### $Id: redirect.m4,v 8.15 1999/08/06 01:47:36 gshapiro Exp $ #####  
44  
45 ##### $Id: always_add_domain.m4,v 8.9 1999/02/07 07:26:08 gshapiro Exp $ #####  
46  
47 ##### $Id: use_cw_file.m4,v 8.9 1999/02/07 07:26:13 gshapiro Exp $ #####  
48  
49  
50 ##### $Id: use_ct_file.m4,v 8.9 1999/02/07 07:26:13 gshapiro Exp $ #####  
51  
52  
53 ##### $Id: local_procmail.m4,v 8.21 1999/11/18 05:06:23 ca Exp $ #####  
54  
55 ##### $Id: access_db.m4,v 8.15 1999/07/22 17:55:34 gshapiro Exp $ #####  
56  
57 ##### $Id: blacklist_recipients.m4,v 8.13 1999/04/02 02:25:13 gshapiro Exp $ #####  
58  
59  
60 ##### $Id: accept_unresolvable_domains.m4,v 8.10 1999/02/07 07:26:07 gshapiro Exp $  
#####
```



```
root@flash:~  
檔案 編輯 Settings 說明  
61 Cwlocalhost.localdomain  
62  
63  
64 ##### $Id: proto.m4,v 8.446.2.5.2.44 2001/07/31 22:25:49 gshapiro Exp $ #####  
65  
66  
67 # level 9 config file format  
68 V9/Berkeley  
69  
70 # override file safeties - setting this option compromises system security,  
71 # addressing the actual file configuration problem is preferred  
72 # need to set this before any file actions are encountered in the cf file  
73 #0 DontBlameSendmail=safe  
74  
75 # default LDAP map specification  
76 # need to set this now before any LDAP maps are defined  
77 #0 LDAPDefaultSpec=-h localhost  
78  
79 #####  
80 # local info #  
81 #####  
82  
83 Cwlocalhost  
84 # file containing names of hosts for which we receive email  
85 Fw/etc/mail/local-host-names  
86  
87 # my official domain name  
88 # ... define this only if sendmail cannot automatically determine your domain  
89 Dj$w.Foo.COM  
90
```

```
root@flash:~  
檔案 編輯 Settings 說明  
91 CP.  
92  
93 # "Smart" relay host (may be null)  
94 DS  
95  
96  
97 # operators that cannot be in local usernames (i.e., network indicators)  
98 CO @ % !  
99  
100 # a class with just dot (for identifying canonical names)  
101 C..  
102  
103 # a class with just a left bracket (for identifying domain literals)  
104 C[[  
105  
106 # access_db acceptance class  
107 C{Accept}OK RELAY  
108  
109  
110  
111  
112 # Hosts for which relaying is permitted ($=R)  
113 FR-o /etc/mail/relay-domains  
114  
115 # arithmetic map  
116 Karith arith  
117 # possible values for tls_connect in access map  
118 C{tls}VERIFY ENCR  
119  
120 # who I send unqualified names to (null means deliver locally)
```



```
root@flash:~  
檔案 編輯 Settings 說明  
121 DR  
122  
123 # who gets all local email traffic ($R has precedence for unqualified names)  
124 DH  
125  
126 # dequoting map  
127 Kdequote dequote  
128  
129 # class E: names that should be exposed as from this host, even if we masquerade  
130 # class L: names that should be delivered locally, even if we have a relay  
131 # class M: domains that should be converted to $M  
132 # class N: domains that should not be converted to $M  
133 #CL root  
134 C(E)root  
135  
136 # who I masquerade as (null for no masquerading) (see also $=M)  
137 DM  
138  
139 # my name for error messages  
140 DnMAILER-DAEMON  
141  
142  
143 # Mailer table (overriding domains)  
144 Kmailertable hash -o /etc/mail/mailertable.db  
145  
146 # Virtual user table (maps incoming users)  
147 Kvirtuser hash -o /etc/mail/virtusertable.db  
148  
149 CPREDIRECT  
150 □
```

```
root@flash:~  
檔案 編輯 Settings 說明  
151 # Access list database (for spam stomping)  
152 Kaccess hash -o /etc/mail/access.db  
153  
154 # Configuration version number  
155 DZ8.11.6  
156  
157  
158 #####  
159 # Options #  
160 #####  
161  
162 # strip message body to 7 bits on input?  
163 0 SevenBitInput=False  
164  
165 # 8-bit data handling  
166 #0 EightBitMode=pass8  
167  
168 # wait for alias file rebuild (default units: minutes)  
169 0 AliasWait=10  
170  
171 # location of alias file  
172 0 AliasFile=/etc/aliases  
173  
174 # minimum number of free blocks on filesystem  
175 0 MinFreeBlocks=100  
176  
177 # maximum message size  
178 #0 MaxMessageSize=1000000  
179  
180 # substitution for space (blank) characters
```



```
root@flash:~  
檔案 編輯 Settings 說明  
181  BlankSub=  
182  
183 # avoid connecting to "expensive" mailers on initial submission?  
184  HoldExpensive=False  
185  
186 # checkpoint queue runs after every N successful deliveries  
187 #0 CheckpointInterval=10  
188  
189 # default delivery mode  
190  DeliveryMode=background  
191  
192 # automatically rebuild the alias database?  
193 # NOTE: There is a potential for a denial of service attack if this is set.  
194 # This option is deprecated and will be removed from a future version.  
195  AutoRebuildAliases  
196  
197 # error message header/file  
198 #0 ErrorHeader=/etc/mail/error-header  
199  
200 # error mode  
201 #0 ErrorMode=print  
202  
203 # save Unix-style "From_" lines at top of header?  
204 #0 SaveFromLine=False  
205  
206 # temporary file mode  
207  TempFileMode=0600  
208  
209 # match recipients against GECOS field?  
210  MatchGECOS=False
```

```
root@flash:~  
檔案 編輯 Settings 說明  
211  
212 # maximum hop count  
213 #0 MaxHopCount=17  
214  
215 # location of help file  
216  HelpFile=/etc/mail/helpfile  
217  
218 # ignore dots as terminators in incoming messages?  
219 #0 IgnoreDots=False  
220  
221 # name resolver options  
222 #0 ResolverOptions=+AAONLY  
223  
224 # deliver MIME-encapsulated error messages?  
225  SendMimeErrors=True  
226  
227 # Forward file search path  
228  ForwardPath=$z/.forward.$w:$z/.forward  
229  
230 # open connection cache size  
231  ConnectionCacheSize=2  
232  
233 # open connection cache timeout  
234  ConnectionCacheTimeout=5m  
235  
236 # persistent host status directory  
237 #0 HostStatusDirectory=.hoststat  
238  
239 # single thread deliveries (requires HostStatusDirectory)?  
240  SingleThreadDelivery=False
```



```
root@flash:~  
檔案 編輯 Settings 說明  
241  
242 # use Errors-To: header?  
243  UseErrorsTo=False  
244  
245 # log level  
246  LogLevel=9  
247  
248 # send to me too, even in an alias expansion?  
249  MeToo=True  
250  
251 # verify RHS in newaliases?  
252  CheckAliases=False  
253  
254 # default messages to old style headers if no special punctuation?  
255  OldStyleHeaders=True  
256  
257 # SMTP daemon options  
258  
259  DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA  
260  
261 # SMTP client options  
262  ClientPortOptions=Address=0.0.0.0  
263  
264 # privacy flags  
265  PrivacyOptions=authwarnings,nowr-fy,noexrn,restrictqrun  
266  
267 # who (if anyone) should get extra copies of error messages  
268  PostmasterCopy=Postmaster  
269  
270  slope of queue-only function
```

```
root@flash:~  
檔案 編輯 Settings 說明  
271  QueueFactor=600000  
272  
273 # queue directory  
274  QueueDirectory=/var/spool/mqueue  
275  
276 # timeouts (many of these)  
277  Timeout.initial=5m  
278  Timeout.connect=1m  
279  Timeout.icconnect=5m  
280  Timeout.helo=5m  
281  Timeout.mail=10m  
282  Timeout.rcpt=1h  
283  Timeout.datainit=5m  
284  Timeout.datablock=1h  
285  Timeout.datafinal=1h  
286  Timeout.rset=5m  
287  Timeout.quit=2m  
288  Timeout.misc=2m  
289  Timeout.command=1h  
290  Timeout.ident=5s  
291  Timeout.fileopen=60s  
292  Timeout.control=2m  
293  Timeout.queuereturn=5d  
294  Timeout.queuereturn.normal=5d  
295  Timeout.queuereturn.urgent=2d  
296  Timeout.queuereturn.non-urgent=7d  
297  Timeout.queuewarn=4h  
298  Timeout.queuewarn.normal=4h  
299  Timeout.queuewarn.urgent=1h  
300  Timeout.queuewarn.non-urgent=12h
```



第 172 行定義 aliases 檔的位置

```
171 # location of alias file  
172 0 AliasFile=/etc/aliases
```

第 175 行定義了最小的剩餘磁碟區塊

```
174 # minimum number of free blocks on filesystem  
175 0 MinFreeBlocks=100
```

第 178 行定義了 ESMTP 訊息的最大長度。

```
177 # maximum message size  
178 #0 MaxMessageSize=1000000
```

第 212 行定義了設定網站的跳躍計數的最大值

```
212 # maximum hop count  
213 #0 MaxHopCount=17
```

第 231 行定義了多重 SMTP 連線。

```
230 # open connection cache size  
231 0 ConnectionCacheSize=2
```

我們將第 264 行的 Addr 位置設定成我們郵件主機的位置,這樣就可以使用 SMTP 接收郵件了。

```
262 # SMTP daemon options  
263  
264 0 DaemonPortOptions=Port=smtp,Addr=61.218.29.3, Name=MTA
```

第 268 行定義了郵件管理員的郵件複本。

```
267 # who (if anyone) should get extra copies of error messages  
268 #0 PostmasterCopy=Postmaster
```

第 271 行定義了高負荷時是否將郵件放入的額外複本。

```
270 # slope of queue-only function  
271 #0 QueueFactor=600000
```

第 274 行定義了放置佇列目錄的位置。

```
273 # queue directory  
274 0 QueueDirectory=/var/spool/mqueue
```

第 388 行定義了能處理最大佇列的訊息。



```
387 # how many jobs can you process in the queue?
388 #0 MaxQueueRunSize=10000
```

<<5>>sendmail 的組態命令

#	註解，那一行會被忽列
C	定義一個類型巨集
D	定義一個巨集
E	提供給代理程式的環境
F	定義一個檔案或管線取得的類型巨集
H	定義一個標頭
K	建立一個具有鍵值對應的對應項目
M	定義一個郵件遞送代理程式
O	定義一個選項
P	定義遞送優先權
R	定義一個轉換規則
S	選告一個規則的開始

29-1-1 組態自己系統的郵件伺服器

我們可以使用 m4 指令按造 sendmail.mc 組態自己的郵件系統，先備份郵件伺服器的組態檔/etc/mail/sendmail.cf 到/home/chaiyen 的目錄下，然後我們可以用 m4 指令產生一個新的組態檔，然後再重新啟動。

```
[root@flash chaiyen]# cp /etc/mail/sendmail.cf /home/chaiyen
[root@flash chaiyen]# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
[root@flash chaiyen]# /sbin/chkconfig sendmail --level 235 on
[root@flash chaiyen]# /etc/rc.d/init.d/sendmail restart
```



29-2 pop 與 imap 伺服器

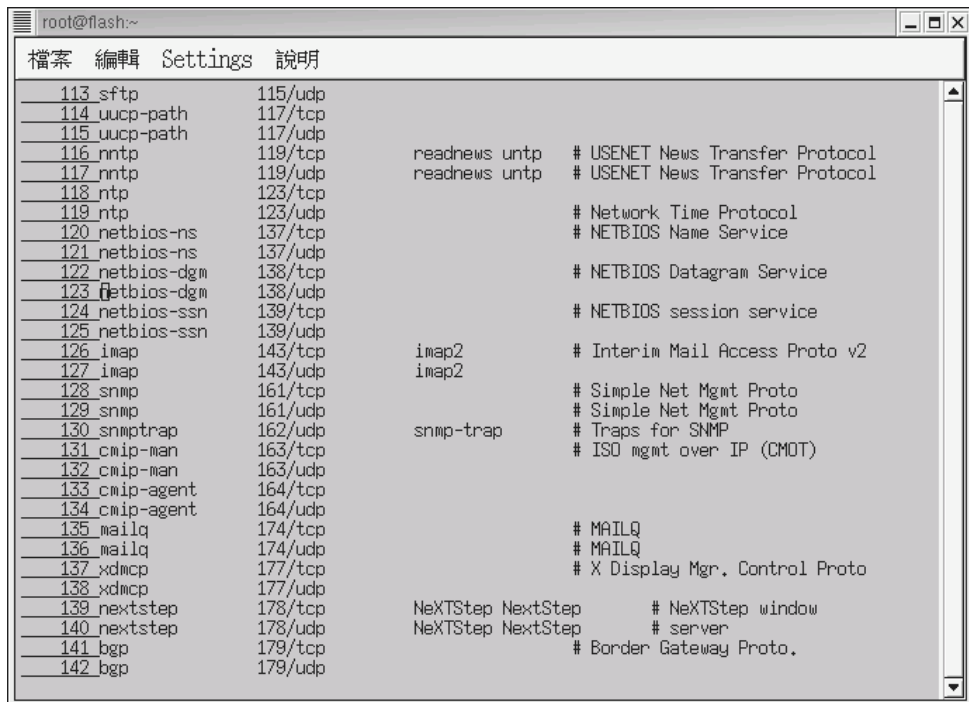
<<1>>pop 與 imap 伺服器

我們要在郵件主機上加上 pop server 與 imap server 的功能，這樣使用者才可以將電子郵件從網站的主機取回。Pop 與 imap 伺服器就像是郵局一樣可以讓我們在郵局收發郵件。這其中的差別是，POP3 不需要以 Web 為基礎，但 IMAP 需要以 Web 為基礎來收發 e-mail。

我們要編輯系統的服務，將 pop 及 imap 的註解符號 # 去除

```
[root@aasir /root]# vi /etc/services
```

第 126 行和第 127 行為啟動 imap 服務



```
root@flash:~
檔案 編輯 Settings 說明
113_sftp      115/udp
114_uucp-path 117/tcp
115_uucp-path 117/udp
116_nntp     119/tcp
117_nntp     119/udp
118_ntp      123/tcp
119_ntp      123/udp
120_netbios-ns 137/tcp
121_netbios-ns 137/udp
122_netbios-dgm 138/tcp
123_netbios-dgm 138/udp
124_netbios-ssn 139/tcp
125_netbios-ssn 139/udp
126_imap     143/tcp
127_imap     143/udp
128_snmp     161/tcp
129_snmp     161/udp
130_snmptrap 162/udp
131_cyip-man 163/tcp
132_cyip-man 163/udp
133_cyip-agent 164/tcp
134_cyip-agent 164/udp
135_mailq   174/tcp
136_mailq   174/udp
137_xdmcp   177/tcp
138_xdmcp   177/udp
139_nextstep 178/tcp
140_nextstep 178/udp
141_bgp     179/tcp
142_bgp     179/udp
readnews untp # USENET News Transfer Protocol
readnews untp # USENET News Transfer Protocol
# Network Time Protocol
# NETBIOS Name Service
# NETBIOS Datagram Service
imap2       # Interim Mail Access Proto v2
imap2
# Simple Net Mgmt Proto
# Simple Net Mgmt Proto
snmp-trap  # Traps for SNMP
# ISO mgmt over IP (CMOT)
# MAILQ
# MAILQ
# X Display Mgr. Control Proto
NeXTStep NextStep # NeXTStep window
NeXTStep NextStep # server
# Border Gateway Proto.
```


第 163 和 164 行為啟動 imap3 服務。

```

root@flash~
檔案 編輯 Settings 說明
155 at-zis 206/tcp # AppleTalk zone information
156 at-zis 206/udp
157 qmt 209/tcp # Quick Mail Transfer Protocol
158 qmt 209/udp # Quick Mail Transfer Protocol
159 z39.50 210/tcp # NISO Z39.50 database
160 z39.50 210/udp z3950 wais
161 ipx 213/tcp # IPX
162 ipx 213/udp
163 imap3 220/tcp # Interactive Mail Access
164 imap3 220/udp # Protocol v3
165 link 245/tcp ttyslink
166 link 245/udp ttyslink
167 rsvp_tunnel 363/tcp
168 rsvp_tunnel 363/udp
169 rpc2portmap 369/tcp
170 rpc2portmap 369/udp # Coda portmapper
171 codaaauth2 370/tcp
172 codaaauth2 370/udp # Coda authentication server
173 ulistproc 372/tcp ulistserv # UNIX Listserv
174 ulistproc 372/udp ulistserv
175 ldap 389/tcp
176 ldap 389/udp
177 svrloc 427/tcp # Server Location Protocol
178 svrloc 427/udp # Server Location Protocol
179 mobileip-agent 434/tcp
180 mobileip-agent 434/udp
181 mobilip-mn 435/tcp
182 mobilip-mn 435/udp
183 https 443/tcp # MCom
184 fhttps 443/udp # MCom

```

第 244 和 245 行為啟動 pop3 服務。

```

root@flash~
檔案 編輯 Settings 說明
234 phonebook 767/tcp # Network phonebook
235 phonebook 767/udp
236 rsync 873/tcp # rsync
237 rsync 873/udp # rsync
238 telnets 992/tcp
239 telnets 992/udp
240 imaps 993/tcp # IMAP over SSL
241 imaps 993/udp # IMAP over SSL
242 ircs 994/tcp
243 ircs 994/udp
244 pop3s 995/tcp # POP-3 over SSL
245 pop3s 995/udp # POP-3 over SSL
246 #
247 #
248 # UNIX specific services
249 #
250 exec 512/tcp
251 biff 512/udp cwsat
252 login 513/tcp
253 who 513/udp whod
254 shell 514/tcp cwd # no passwords used
255 syslog 514/udp
256 printer 515/tcp spooler # line printer spooler
257 printer 515/udp spooler # line printer spooler
258 talk 517/udp
259 ntalk 518/udp
260 utime 519/tcp unixtime
261 utime 519/udp unixtime
262 efs 520/tcp
263 rrouter 520/udp route routed # RIP

```



29-2-1 修改 imap 檔案

我們使用 vi 編輯/etc/xinetd.d/imap 來編輯 imap 檔案。

```
[root@flash /]# vi /etc/xinetd.d/imap
```

我們將第七行的 disable 設為 no，這樣就可以啟動 imap 服務。

```
1 # default: off
2 # description: The IMAP service allows remote users to access their mail
  using \
3 #           an IMAP client such as Mutt, Pine, fetchmail, or Netscape
  \
4 #           Communicator.
5 service imap
6 {
7     disable = no
8     socket_type          = stream
9     wait                 = no
10    user                  = root
11    server                 = /usr/sbin/imapd
12    log_on_success        += HOST DURATION
13    log_on_failure        += HOST
14 }
```

29-2-2 修改 ipop3 檔案

我們使用 vi 編輯/etc/xinetd.d/ipop3 來編輯 ipop3 檔案。

```
[root@flash /]# vi /etc/xinetd.d/ipop3
```

我們將第七行的 disable 設為 no，這樣就可以啟動 pop3 服務。

```
1 # default: off
2 # description: The POP3 service allows remote users to access their mail
  \
3 #           using an POP3 client such as Netscape Communicator, mutt,
  \
4 #           or fetchmail.
5 service pop3
6 {
7     disable = no
8     socket_type          = stream
9     wait                 = no
10    user                  = root
11    server                 = /usr/sbin/ipop3d
12    log_on_success        += HOST DURATION
13    log_on_failure        += HOST
14 }
```



29-2-3 啟動 SSL 加密

POP3 和 SSL 加密使用在一起，我們需要建立和安裝安全認證。首先我們可以建立我們的認證目錄/etc/mail/certs。

```
# mkdir -p -m665 /etc/mail/certs
# chown root:mail /etc/mail/certs
# chmod 660 /etc/mail/certs
```

我們使用 openssl 來產生認證需求。我們將建立 cert.pem 的私有密鑰，其過程就和 Apache2 使用 SSL 加密一樣。

```
# openssl req -new -nodes -out req.pem -keyout /etc/mail/certs/cert.pem
```

這是填入認證的相關資訊。

```
Generating a 1024 bit RSA private key
...+++++
.....+++++
writing new private key to '/etc/mail/certs/cert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:TW
State or Province Name (full name) [Berkshire]:taipei
Locality Name (eg, city) [Newbury]:taipei
Organization Name (eg, company) [My Company Ltd]:aasir
Organizational Unit Name (eg, section) []:aasir
Common Name (eg, your name or your server's hostname) []:wu.chaiyen
Email Address []:wu.chaiyen@msa.hinet.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:353766aa
An optional company name []:chaiyen
```

```
# chmod 600 /etc/mail/certs/cert.pem
# chown root:0 /etc/mail/certs/cert.pem
```

當我們登錄完認證授權後，我們可以使用將我們的 cert.pem 傳送到認證公司(例如 VeriSign)去授權，它會給我們授權以後的 signed_req.pem，然後我們將認證輸出到/etc/mail/certs/cert.pem。

```
# cat signed_req.pem >> /etc/mail/certs/cert.pem
```



我們的 POP3 其組態檔是放在/etc/log.d/conf/services/in.qpopper.conf 的地方，我們可以修改 qpopper.conf 組態檔。

```
#vi /etc/log.d/conf/services/in.qpopper.conf
```

我們新增 SSL 加密，任何使用者端支援 SSL 將可以安全的方式來連接並下載郵件。

```
set tls-support=stls
```

```
set tls-server-cert-file=/etc/mail/certs/cert.pem
```

這是我們模擬認證授權自己來建立簽證。

首先建立 CA 私有密鑰然後再建立 CA 認證。

```
#openssl genrsa -des3 -out ca.key 1024
```

```
#openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

```
#openssl x509 -req -CA ca.crt -Cakey ca.key -days 365 -in req.pem -out signed_req.pem -Ccreateserial
```

我們可以在 <http://www.eudora.com/qpopper> 上找到相關的資訊。



29-3 DNS 解析

郵件伺服器需要一個正確的 DNS 資訊建立在我們的機器上。假如我們沒有郵件伺服器名稱資訊而只有 IP 位置，這樣可能無法郵寄信件，因為它們可能會被退回。郵件伺服器在預設的組態中設定只接受有完整名稱位置或 DNS 解析名稱的郵件。

我們在建立郵件伺服器前，需先查看我們 DNS 反轉查詢是否正確。我們可以使用 nslookup 指令來查詢，這是查詢我們主機 flash.aasir.com，它的名稱伺服器是 dns.hinet.net 而 ip 位置是 168.95.1.1。

```
[root@aasir mail]# nslookup flash.aasir.com
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead. Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
Server:      168.95.1.1
Address:     168.95.1.1#53

Name:   flash.aasir.com
Address: 61.218.29.3
```

如果我們所查詢的主機不存在，則會發生下面的情況。

```
[root@aasir mail]# nslookup kk.aasir.com
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead. Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
Server:      168.95.1.1
Address:     168.95.1.1#53

** server can't find kk.aasir.com: NXDOMAIN
```



課後練習

1. 何者是 Sendmail 郵件伺服器的組態檔？

- (A). A./etc/mail/sendmail.mc
- (B). B./etc/sendmail.mc
- (C). C./etc/mail/sendmail.cf
- (D). D./etc/sendmail.cf

2. 我們要在郵件主機上加上 POP server 與 IMAP server 的功能，這樣使用者才可以將電子郵件從網站的主機取回。POP 與 IMAP 伺服器就像是郵局一樣可以讓我們在郵局收發郵件。請問何者不需要用到以 Web 為基礎的 e-mail 界面有可以收發郵件？何者允許使用 Web 為基礎的界面來收發 e-mail？

- (A). POP3 不需要以 Web 為基礎,但 IMAP 需要以 Web 為基礎來收發 e-mail
- (B). POP3 需要以 Web 為基礎,但 IMAP 不需要以 Web 為基礎來收發 e-mail
- (C). POP3 需要以 Web 為基礎,且 IMAP 也需要以 Web 為基礎來收發 e-mail
- (D). POP3 不需要以 Web 為基礎,且 IMAP 也不需要以 Web 為基礎來收發 e-mail

3. 我們可以編輯 sendmail 的別名設定，每一個使用者都可以設定多個別名，在哪一個檔案中我們可以設定別名？

- (A). A./etc/aliases
- (B). B. /etc/sendmail.mc
- (C). C. /etc/mail/sendmail.cf
- (D). D./etc/mail/aliases



4. 郵件伺服器需要一個正確的何種資訊建立在我們的機器上？假如我們沒有郵件伺服器的名稱資訊而只有 IP 位置，這樣可能無法郵寄信件，因為它們可能會被退回。郵件伺服器在預設的組態中設定只接受有完整名稱位置或該解析名稱的郵件。
- (A). DNS
 - (B). mail
 - (C). MTA
 - (D). MUA

-
5. 當使用者使用 Outlook 來發送已經寫好的電子郵件(這邊稱為 Mail User Agent 郵件使用者代理 MUA)，這個 message 訊息會傳送到 SMTP 伺服器的郵件訊息佇列 Message Queue(這邊稱為 Mail Transfer Agent 郵件傳輸代理 MTA)。當郵件傳送代理一收到這個電子郵件，就會立刻轉信(relay)到相關的郵件傳送代理 MTA，並且放到該地址的使用者郵件信箱。在這遠端的郵件傳輸代理 MTA，它放置這郵件到使用者的郵件信箱，它可以被本地端連線的使用者讀取，也可以被遠端的使用者透過 POP3 的協定來收信。我們當 RedHat Linux Fadora 1 的管理者要知道郵件伺服器 Sendmail 的操作方式就是使用何者郵件傳輸代理？使用者使用 Outlook 來收發電子郵件，這是使用何種方式？

【答案】

1.C 2.C 3.A 4.A 5.MTA、MUA



NOTE

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

