Postfix

lctseng / Liang-Chi Tseng

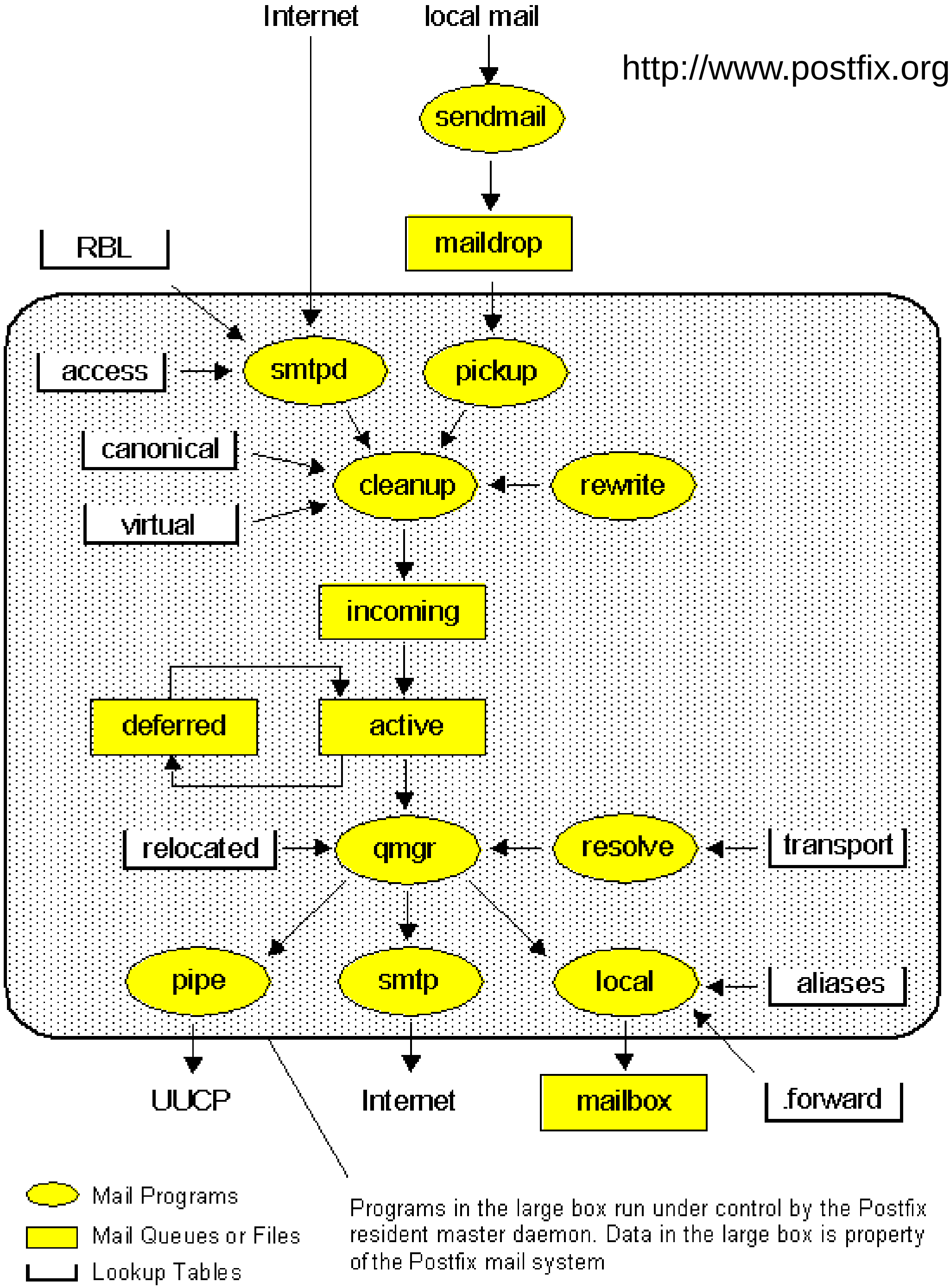
Outline

- A very long topic
- Step-by-step examples after brief introduction
- Outline
  - Brief introduction to Postfix
  - Step by step examples
    - Build a basic MTA that can send mails to other domain
      - Clients from localhost only
    - Add authentication to MTA so that other host can send with your host
    - Add encryption
    - Basic MTA/MDA/MAA that you can receive mails from other domain
  - Detailed Postfix configuration

Postfix

- ❑Free and open source mail transfer agent (MTA)
  - For the routing and delivery of email
  - Intended as a fast, easy-to-administer, and secure alternative to the widely-used Sendmail
  - Formerly VMailer / IBM Secure Mailer
    - By Wietse Venema at the IBM Thomas J. Watson Research Center
  - IBM Public License
- ❑First released in mid-1999
- ❑http://www.postfix.org
  - http://www.postfix.org/documentation.html

http://www.postfix.org/OVERVIEW.html

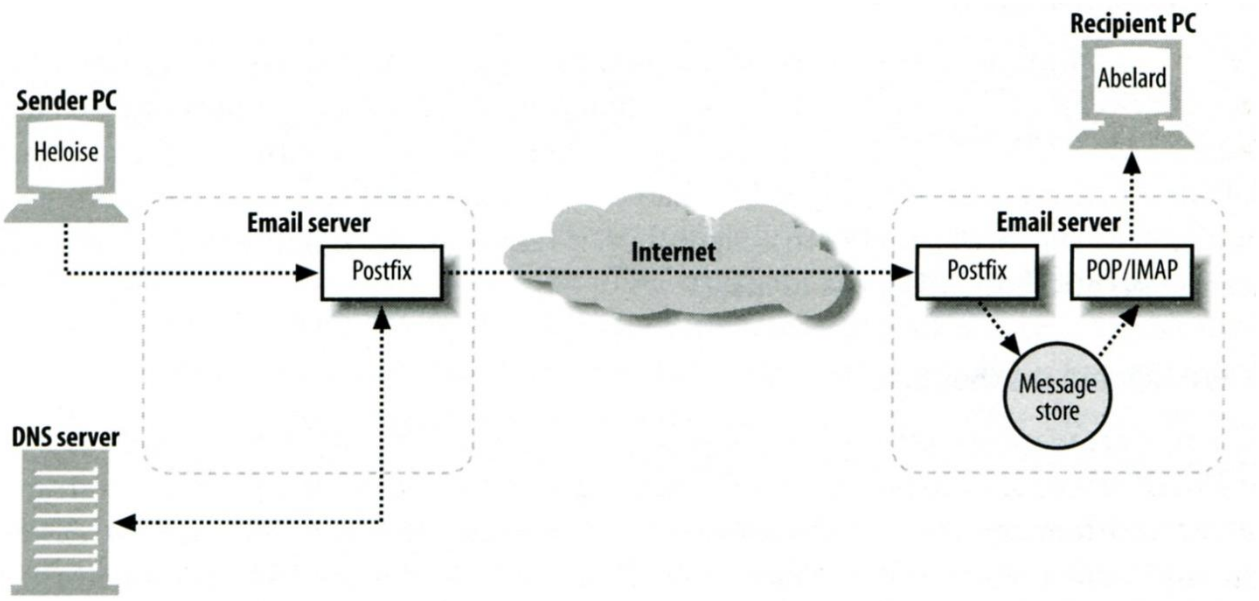


Programs in the large box run under control by the Postfix resident master daemon. Data in the large box is property of the Postfix mail system

Role of Postfix

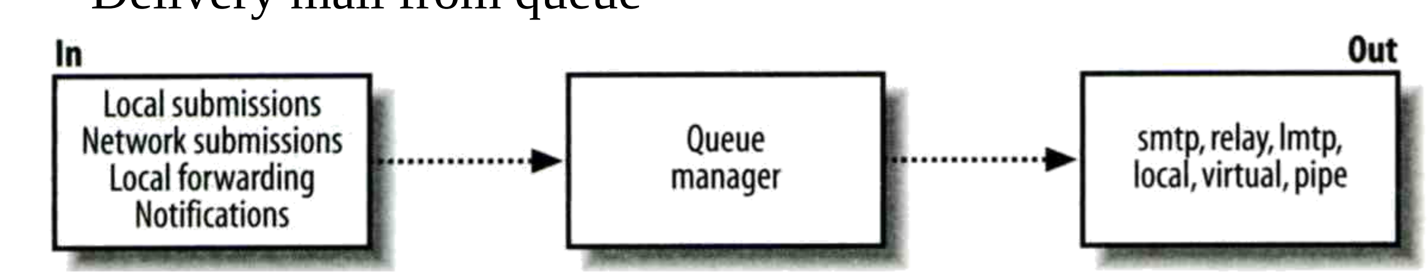
❑ MTA that

- Receive and deliver email over the network via SMTP
- Local delivery directly or use other mail delivery agent



Postfix Architecture

- ❑ Modular-design MTA
  - Not like sendmail of monolithic system
  - Decompose into several individual program that each one handle specific task
  - The most important daemon: `master` daemon
    - ➢ Reside in memory
    - ➢ Get configuration information from master.cf and main.cf
    - ➢ Invoke other process to do jobs
- ❑ Major tasks
  - Receive mail and put in queue
  - Queue management
  - Delivery mail from queue



In

Local submissions
Network submissions
Local forwarding
Notifications

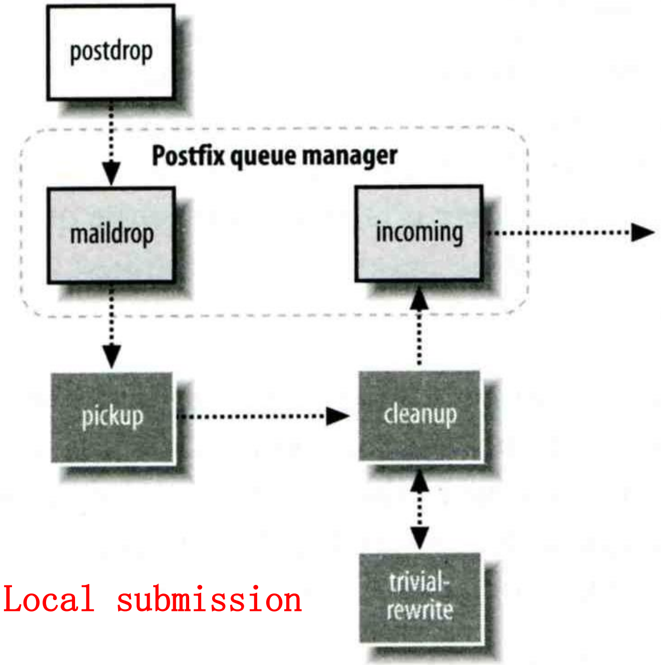
Queue manager

smtp, relay, lmtp, local, virtual, pipe

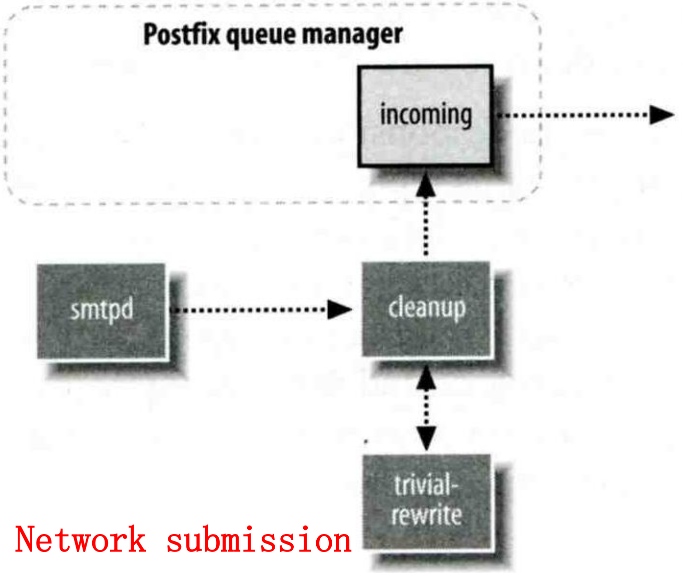
Out

Postfix Architecture – Message IN

- Four ways
  - Local submission
    - postdrop command
    - maildrop directory
    - pickup daemon
    - cleanup daemon
      - Header validation
      - address translation
    - incoming directory
  - Network submission
    - smtpd daemon
  - Local forwarding
    - Resubmit for such as .forward
  - Notification
    - defer daemon
    - bounce daemon



Local submission



Network submission

Postfix Architecture – Queue

- ❑ Five different queues
  - incoming
    - ➢ The first queue that every incoming email will stay
  - active
    - ➢ Queue manager will move message into active queue whenever there is enough system resources
    - ➢ Queue manager then invokes suitable DA to delivery it
  - deferred
    - ➢ Messages that cannot be delivered are moved here
    - ➢ These messages are sent back either with bounce or defer daemons
  - corrupt
    - ➢ Used to store damaged or unreadable message
  - hold

http://www.postfix.org/QSHAPE_README.html#queues

Postfix Architecture – Message OUT (1)

- ❑ Address classes
  - Used to determine which destinations to accept for delivery
  - How the delivery take place
- ❑ Main address classes
  - Local delivery
    - ➢ Domain names in "mydestination" is local delivered
    - ➢ Ex:
      - – mydestination = nabsd.cs.nctu.edu.tw localhost
    - ➢ It will check alias and .forward file to do further delivery
  - Virtual alias
    - ➢ Ex:
      - – virtual-alias.domain
      - – user1@virtual-alias.domain address1
  - Virtual mailbox
    - ➢ Each recipient address can have its own mailbox
    - ➢ Ex:
      - – virtual_mailbox_base = /var/vmail
      - – /var/mail/vmail/CSIE, /var/mail/vmail/CS
  - Relay
    - ➢ Transfer mail for others to not yours domain
    - ➢ It is common for centralize mail architecture to relay trusted domain
  - Deliver mail to other domain for authorized user
    - ➢ The queue manager will invoke the smtp DA to deliver this mail

Postfix Architecture – Message OUT (2)

❑ Other delivery agent (MDA)

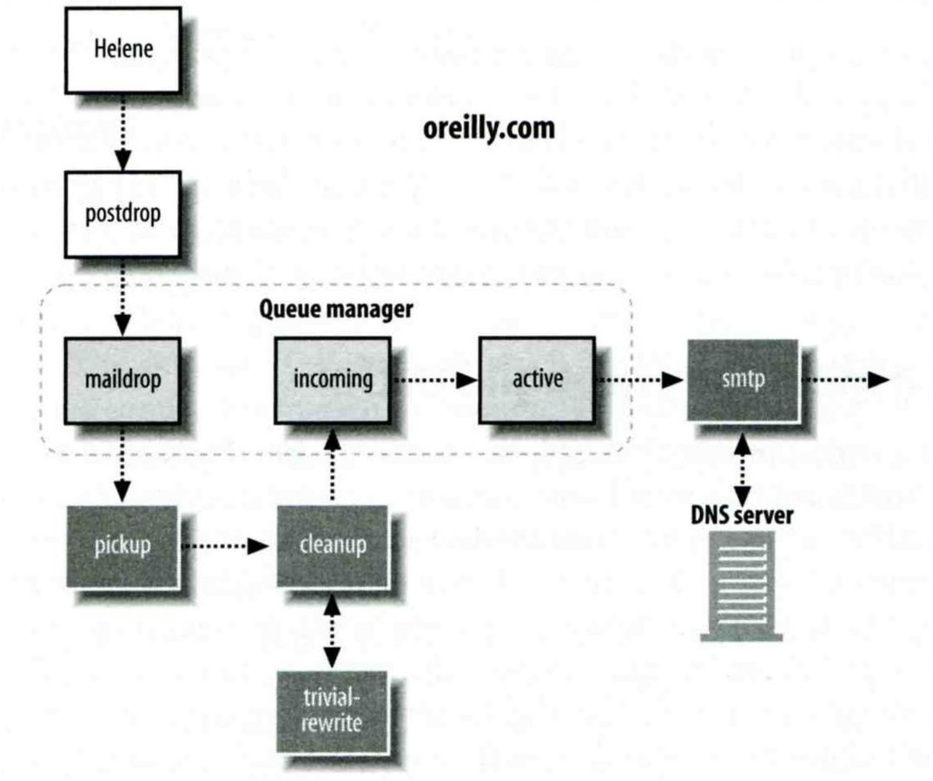
- Specify in /usr/local/etc/postfix/master.cf
  - – How a client program connects to a service and what daemon program runs when a service is requested

```
pickup    fifo  n      -      n      60     1      pickup
cleanup   unix  n      -      n      -      0      cleanup
bounce    unix  -      -      n      -      0      bounce
defer     unix  -      -      n      -      0      bounce
smtp      unix  -      -      n      -      -      smtp
relay     unix  -      -      n      -      -      smtp
```

- lmtp
  - ➢ Local Mail Transfer Protocol
  - ➢ Used for deliveries between mail systems on the same network even the same host
    - – Such as postfix → POP/IMAP to store message in store with POP/IMAP proprietary format
- pipe
  - ➢ Used to deliver message to external program

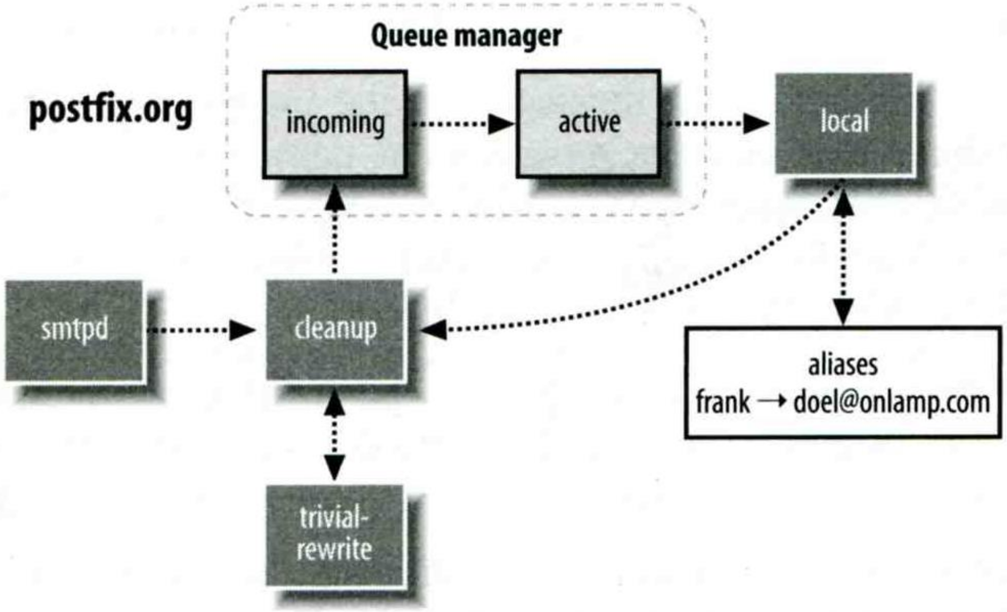
Message Flow in Postfix (1)

- Example
  - helene@oreilly.com → frank@postfix.org (doel@onlamp.com)
  - Phase1:
    - Helene compose mail using her MUA, and then call postfix′s sendmail command to send it



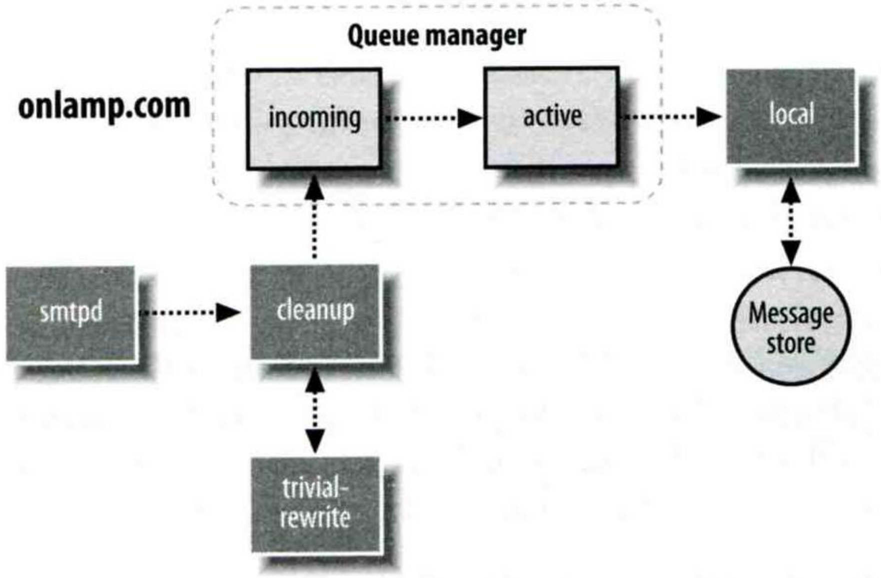
Message Flow in Postfix (2)

- Phase2:
  - The smtpd on postfix.org takes this message and invoke cleanup then put in incoming queue
  - The local DA find that frank is an alias, so it resubmits it through cleanup daemon for further delivery



Message Flow in Postfix (3)

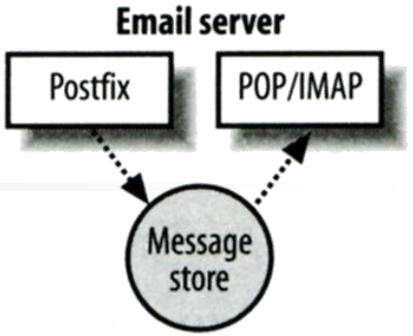
- Phase3
  - The smtpd on onlamp.com takes this message and invoke cleanup then put in incoming queue
  - Local delivery to message store



Message Store Format

- The Mbox format
  - Store messages in single file for each user
  - Each message start with “From ” line and continued with message headers and body
  - Mbox format has file-locking problem
- The Maildir format
  - Use structure of directories to store email messages
  - Each message is in its owned file
  - Three subdirectories
    - cur, new and tmp
  - Maildir format has scalability problem
    - Quick in locating and deleting
- Related parameters (in main.cf)
  - mail_spool_directory = /var/spool/mail (Mbox)
  - mail_spool_directory = /var/spool/mail/ (Maildir)

Postfix and POP/IMAP

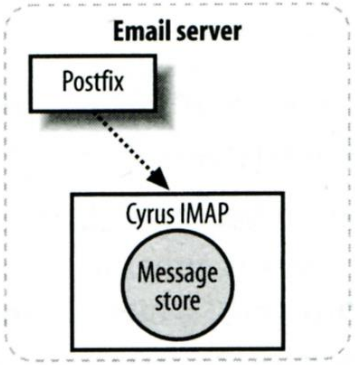


❑ POP vs. IMAP

- Both are used to retrieve mail from server for remote clients
- POP has to download entire message, while IMAP can download headers only
- POP can download only single mailbox, while IMAP can let you maintain multiple mailboxes and folders on server

❑ Cooperation between Postfix and POP/IMAP

- Postfix and POP/IMAP must agree on the type of mailbox format and style of locking
  - ➢ Standard message store
  - ➢ Unstandard message store (using LMTP)
    - – Such as Cyrus IMAP or Dovecot



Postfix Configuration

❑ Two most important configuration files

- /usr/local/etc/postfix/main.cf
  - ➢ Core configuration
- /usr/local/etc/postfix/master.cf
  - ➢ Which postfix service should invoke which program

❑ Edit configuration file

- Using text editor
- postconf
  - ➢ % postconf –e myhostname=nabsd.cs.nctu.edu.tw
  - ➢ % postconf –d myhostname (print default setting)
  - ➢ % postconf myhostname (print current setting)

❑ Reload postfix whenever there is a change

- # postfix reload
- # /usr/local/etc/rc.d/postfix reload

Step by Step Examples

Let’s learn from examples

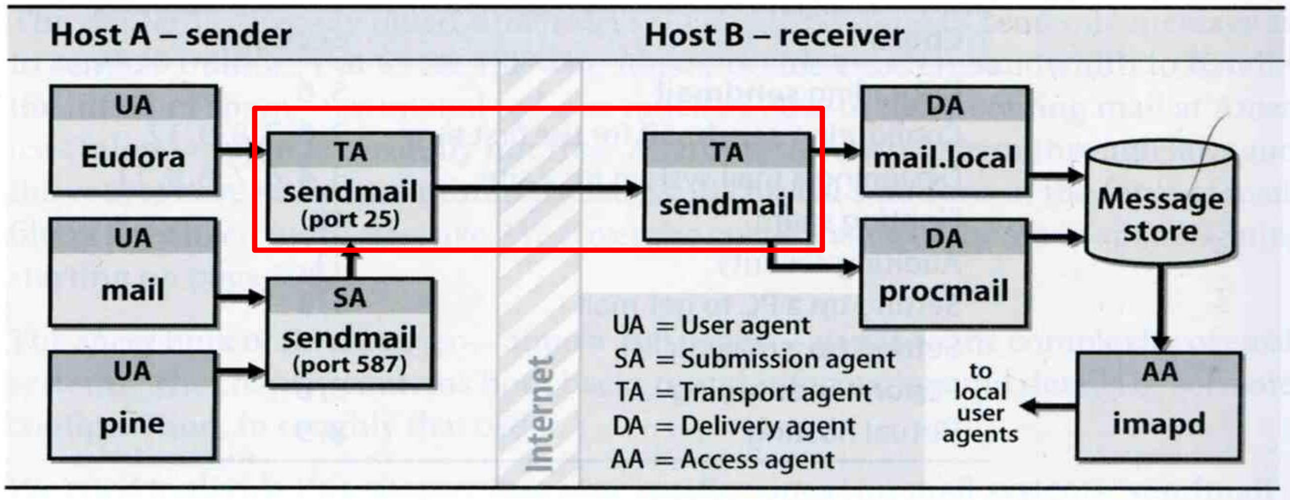
Step by Step Examples

- ❑ Build a Basic MTA
  - Send test mails to verify your MTA
  - Check whether your mail is sent or not
- ❑ MTA Authentication
- ❑ MTA Encryption
- ❑ MAA for POP3 and IMAP

Build a Basic MTA

Can send mails to other domain

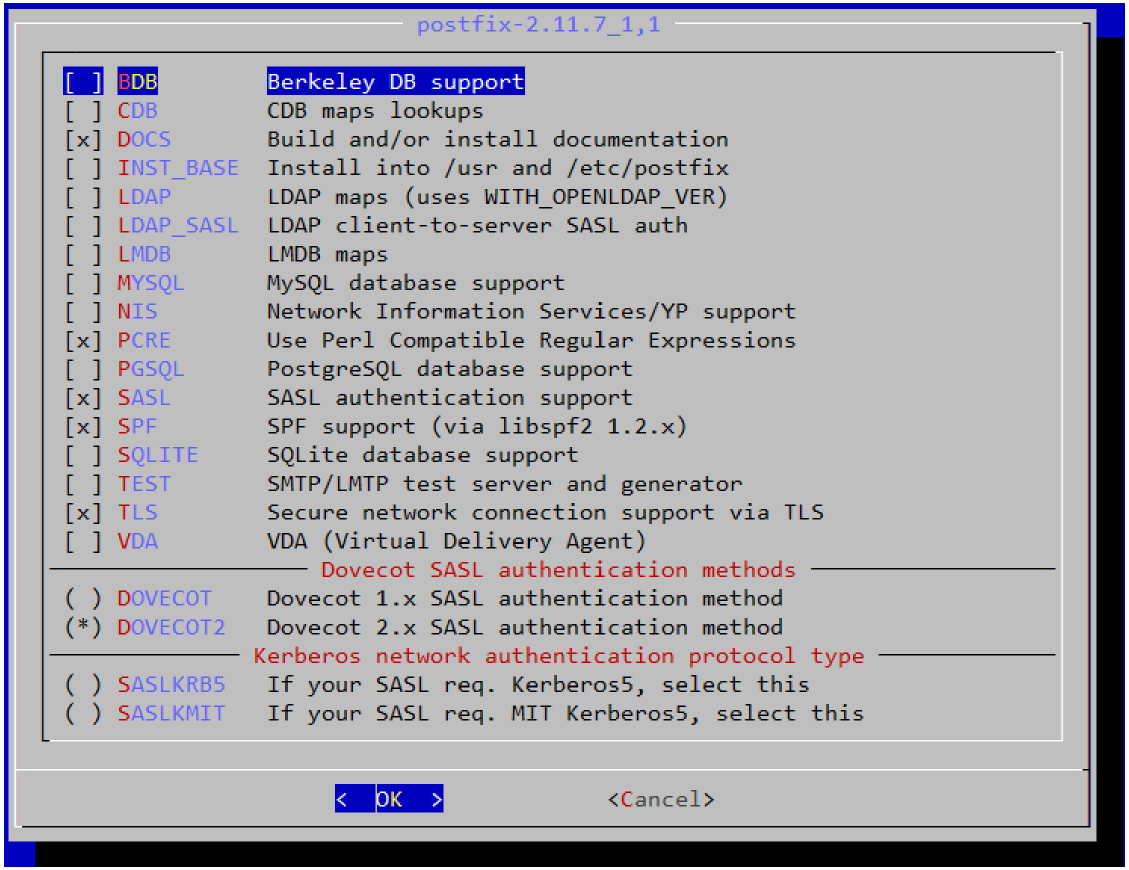
Mail system components



UA = User agent
SA = Submission agent
TA = Transport agent
DA = Delivery agent
AA = Access agent

Build a basic MTA(1)

- ❑ Can send mails to other domain
- ❑ Install Postfix from port (need customization) (version 2.11)
  - mail/postfix
    - ➢ mail/postfix211
  - SASL
  - DOVECOT2



```
                    postfix-2.11.7_1,1
 [ ] BDB        Berkeley DB support
 [ ] CDB        CDB maps lookups
 [x] DOCS       Build and/or install documentation
 [ ] INST_BASE  Install into /usr and /etc/postfix
 [ ] LDAP       LDAP maps (uses WITH_OPENLDAP_VER)
 [ ] LDAP_SASL  LDAP client-to-server SASL auth
 [ ] LMDB       LMDB maps
 [ ] MYSQL      MySQL database support
 [ ] NIS        Network Information Services/YP support
 [x] PCRE       Use Perl Compatible Regular Expressions
 [ ] PGSQL      PostgreSQL database support
 [x] SASL       SASL authentication support
 [x] SPF        SPF support (via libspf2 1.2.x)
 [ ] SQLITE     SQLite database support
 [ ] TEST       SMTP/LMTP test server and generator
 [x] TLS        Secure network connection support via TLS
 [ ] VDA        VDA (Virtual Delivery Agent)
 ────────────── Dovecot SASL authentication methods ──────────────
 ( ) DOVECOT    Dovecot 1.x SASL authentication method
 (*) DOVECOT2   Dovecot 2.x SASL authentication method
 ────────── Kerberos network authentication protocol type ──────────
 ( ) SASLKRB5   If your SASL req. Kerberos5, select this
 ( ) SASLKMIT   If your SASL req. MIT Kerberos5, select this

                 <  OK  >            <Cancel>
```

Build a basic MTA(2)

- The default version of Postfix is changed to 3.1
- You can install them from package
- There may be some compatibility issue
  - All configuration in this slide is based on Postfix 2.11
  - Postfix can run in backwards-compatible mode
- Reference:
  http://www.postfix.org/COMPATIBILITY_README.html

Build a basic MTA(3)

- ❑ During installation
  - Would you like to activate Postfix in /etc/mail/mailer.conf [n]?
  - Answer “y” here
- ❑ After installation
  - Disable “sendmail” program
    - ➢ service sendmail stop
    - ➢ In /etc/rc.conf

```
sendmail_enable="NONE"
```

    - ➢ In /etc/periodic.conf (create if not exists)

```
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"
```

Build a basic MTA(4)

- ❑ After installation
  - Enable postfix
    - ➢ Edit /etc/rc.conf

      ```
      postfix_enable="YES"
      ```

    - ➢ service postfix start
- ❑ Set up DNS records
  - Some domains will reject mails from hosts without DNS record
  - Suppose the hostname is “demo1.nasa.lctseng.nctucs.net”
  - Set up these records
    - ➢ (A record) demo1.nasa.lctseng.nctucs.net
    - ➢ (A record) nasa.lctseng.nctucs.net
    - ➢ (MX record) nasa.lctseng.nctucs.net
      - – Points to “demo1.nasa.lctseng.nctucs.net”

Build a basic MTA(5)

- ❑ Set up MTA identity
  - See Postfix Configuration: MTA identity
  - In main.cf

```
myhostname = demo1.nasa.lctseng.nctucs.net
mydomain = nasa.lctseng.nctucs.net
myorigin = $myhostname
mydestination = $myhostname, localhost.$mydomain,
          localhost, $mydomain
```

- ❑ Reload or restart postfix to apply changes
  - postfix reload

Send test mails to verify your MTA(1)

- “telnet” or “mail” command

```
> telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
EHLO localhost
250-demo1.nasa.lctseng.nctucs.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: lctseng@nasa.lctseng.nctucs.net
250 2.1.0 Ok
RCPT TO: lctseng@cs.nctu.edu.tw
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: This is test mail

DATA
.
250 2.0.0 Ok: queued as 3C868150
```

telnet

Send test mails to verify your MTA(2)

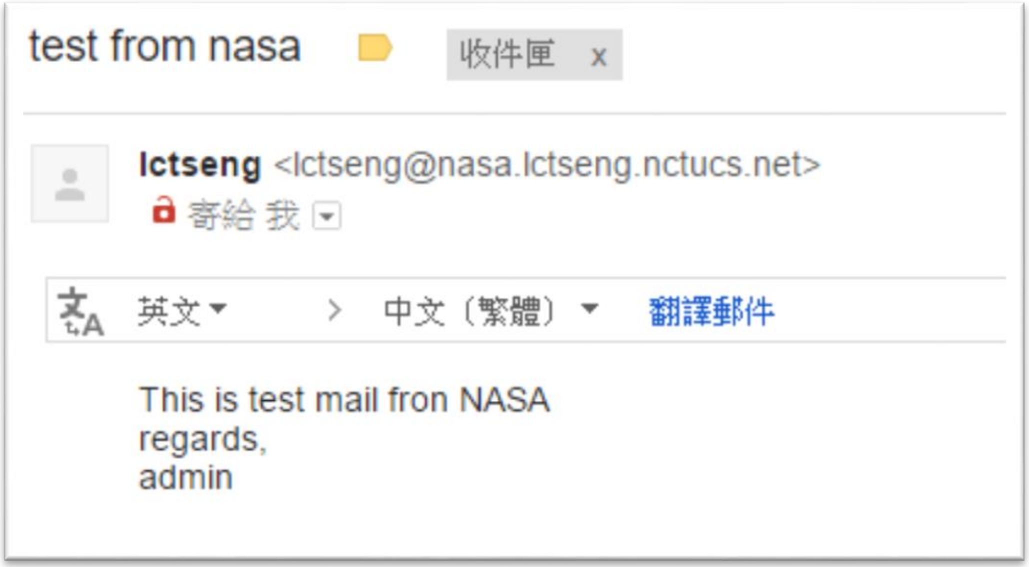
- ❑ The “mail” command

```
> mail -s "test from nasa" lctseng@gmail.com
This is test mail from NASA
regards,
admin
(Press Ctrl+D)
```

mail

- See man page for more details

- ❑ Result (gmail)



test from nasa

lctseng <lctseng@nasa.lctseng.nctucs.net>

This is test mail fron NASA
regards,
admin

Send test mails to verify your MTA(3)

- ❑ Mail source text of last example

```
Delivered-To: lctseng@gmail.com
Received: by 10.129.125.135 with SMTP id y129csp874822ywc;
        Sun, 6 Mar 2016 02:39:22 -0800 (PST)
X-Received: by 10.98.87.90 with SMTP id l87mr25639644pfb.70.1457260762400;
        Sun, 06 Mar 2016 02:39:22 -0800 (PST)
Return-Path: <lctseng@nasa.lctseng.nctucs.net>
Received: from demo1.nasa.lctseng.nctucs.net …(omitted)
        by mx.google.com with ESMTP id bz6si20406744pad.30.2016.03.06.02.39.21
        for <lctseng@gmail.com>;
        Sun, 06 Mar 2016 02:39:21 -0800 (PST)
Received-SPF: neutral (google.com: 140.113.168.238 is neither permitted …(omitted)
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 140.113.168.238 is neither permitted …(omitted)
Received: by demo1.nasa.lctseng.nctucs.net (Postfix, from userid 1001)
         id 6D916162; Sun,  6 Mar 2016 18:38:04 +0800 (CST)
To: lctseng@gmail.com
Subject: test from nasa
Message-Id: <20160306103804.6D916162@demo1.nasa.lctseng.nctucs.net>
Date: Sun,  6 Mar 2016 18:38:04 +0800 (CST)
From: lctseng@nasa.lctseng.nctucs.net (lctseng)

This is test mail from NASA
regards,
admin
```

Check whether your mail is sent or not (1)

- ❑ Sometimes, we do not receive mails immediately
- ❑ There may be some errors when your MTA sending mails to other domain
- ❑ Mails will stay in queues
  - Contain information about each mail
- ❑ Tools to management mail queues
  - See Postfix Configuration: Queue Management - Queue Tools

Check whether your mail is sent or not (2)

❑ Example for rejected mails

```
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
3C868150        377 Sun Mar  6 18:23:11  lctseng@nasa.lctseng.nctucs.net
(host csmx3.cs.nctu.edu.tw[140.113.235.119] said: 450 4.1.8
<lctseng@nasa.lctseng.nctucs.net>: Sender address rejected: Domain not found
 (in reply to RCPT TO command)) lctseng@cs.nctu.edu.tw

-- 0 Kbytes in 1 Request.
```

- Problem
  - ➢ The destination MX cannot verify the domain of sender host
- Reason
  - ➢ You may forget to set up correct DNS record
- This mail will NOT be delivered until you set up your DNS record

Check whether your mail is sent or not (3)

❑ Example for deferred mails

```
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
3C868150        377 Sun Mar  6 18:23:11  lctseng@nasa.lctseng.nctucs.net
(host csmx1.cs.nctu.edu.tw[140.113.235.104] said: 450 4.2.0
<lctseng@cs.nctu.edu.tw>: Recipient address rejected: Greylisted,
 see http://postgrey.schweikert.ch/help/cs.nctu.edu.tw.html
 (in reply to RCPT TO command))    lctseng@cs.nctu.edu.tw

-- 0 Kbytes in 1 Request.
```

- Problem
  - ➢ The mail is deferred for a short time
- Reason
  - ➢ Destination host wants to examine our server is a spamming host or not
- The mail will be delivered after a short time
  - ➢ Generally within 30 minutes

MTA Authentication

We don’t want unauthorized user to access our MTA

MTA authentication(1)

- In previous example, only localhost can send mail to other domain
- If you try telnet on other host, when you try to send mails to other domain, you will get:

```
> telnet demo1.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to demo1.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
MAIL FROM: lctseng@demo1.nasa.lctseng.nctucs.net
250 2.1.0 Ok
RCPT TO: lctseng@gmail.com
454 4.7.1 <lctseng@gmail.com>: Relay access denied
```

- That is because you have following lines in main.cf

```
mynetworks_style = host
```

  - So Postfix only trust clients from localhost
  - See Postfix Configuration: Relay Control

MTA authentication(2)

- ❑ How to let SMTP clients outside from trust networks get the same privileges as trusted hosts?
  - Can send mails to other domain, not only `$mydestination`
  - We need authentication (account and password)
- ❑ SASL Authentication
  - Simple Authentication and Security Layer
  - RFC 2554, RFC 4954
- ❑ To configure SASL for Postfix, we need another daemon
  - Dovecot SASL (we use it in our example)
  - Cyrus SASL
- ❑ References
  - http://wiki2.dovecot.org/
  - http://www.postfix.org/SASL_README.html

MTA authentication(3) - Dovecot SASL

❑ Installation

- mail/dovecot2
- Should be installed when you install Postfix (dependency)
- Note: dovecot still have version 1.x, but it is obsolete

❑ Enable Dovecot SASL daemon

- In /etc/rc.conf

```
dovecot_enable="YES"
```

- Copy configuration files

```
cp -R /usr/local/etc/dovecot/example-config/* \
                /usr/local/etc/dovecot
```

- Create SSL keys for Dovecot (self-signed or use Let’s Encrypt)
  - ➢ Change path for SSL files in /usr/local/etc/dovecot/conf.d/10-ssl.conf
  - ➢ In fact, these are mainly for POP3s and IMAPs, not SASL in Postfix
- service dovecot start

MTA authentication(4) - Postfix with Dovecot SASL

❑ Set up Dovecot SASL authenticate (using system account)

- In /usr/local/etc/dovecot/conf.d/10-master.conf:

```
service auth {
  ...
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
  ...
}
```

- In /usr/local/etc/dovecot/conf.d/10-auth.conf

```
auth_mechanisms = plain login
```

MTA authentication(5) - Postfix with Dovecot SASL

❑ Set up Dovecot SASL in Postfix

- In main.cf

```
# Set SASL to Dovecot
smtpd_sasl_type = dovecot
# Specify the UNIX socket path
smtpd_sasl_path = private/auth
# Enable SASL
smtpd_sasl_auth_enable = yes
# For client capability
broken_sasl_auth_clients = yes
# Allow SASL authenticated clients
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_destination
```

❑ Restart/Reload Dovecot and Postfix

MTA authentication(6)

❑ Now you can authenticate your identity in SMTP

```
> telnet demo1.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to demo1.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
EHLO linuxhome.cs.nctu.edu.tw
250-demo1.nasa.lctseng.nctucs.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

MTA authentication(7)

- The account and password are encoded in Base64
  - If you have perl installed, suggest your account is test and password is testpassword

```
perl -MMIME::Base64 -e 'print encode_base64("\000test\000testpassword");'
```

  - It will generate encoded account and password
    - For example: AHRlc3QAdGVzdHBhc3N3b3Jk

MTA authentication(8)

- ❑ Use the encoded account and password to authenticate it

```
> telnet demo1.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to demo1.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
AUTH PLAIN AHRlc3QAdGVzdHBhc3N3b3Jk
235 2.7.0 Authentication successful
MAIL FROM: lctseng@nasa.lctseng.nctucs.net
250 2.1.0 Ok
RCPT TO: lctseng@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To: lctseng@gmail.com
Subject: This is authenticated client
Message-Id: <20160307120109.861A9154@demo1.nasa.lctseng.nctucs.net>
Date: Mon,  7 Mar 2016 15:01:09 +0800 (CST)
From: lctseng@demo1.nasa.lctseng.nctucs.net (lctseng)

Test Mail
.
250 2.0.0 Ok: queued as F3D59171
```

MTA Encryption

The Internet is dangerous.
We need to protect ourselves from sniffing.

MTA encryption(1)

- In previous example, all SMTP sessions are in plain text
  - Your encoded authentication information is in danger!
- We need encryption over SSL/TLS
  - Like HTTP can be enhanced to HTTPs
  - Postfix supports two kinds of encryption
    - SMTP over TLS
    - SMTPs
- Before we enable SMTP over TLS (or SMTPs), you need SSL keys and certificates
  - Again, just like HTTPs
  - Self-signed or use Let’s Encrypt
  - You can use the same certificates/keys as Dovecot’s
    - In main.cf

```
smtpd_tls_cert_file = /path/to/cert.pem
smtpd_tls_key_file = /path/to/key.pem
```

MTA encryption(2-1) - Set up SMTP over TLS

- Recommended for SMTP encryption
- Use the same port as SMTP (port 25)
- No force encryption
  - Client can choose whether to encrypt mails or not
  - But server can configured to force encryption
- In main.cf
  - No force encryption

    ```
    smtpd_tls_security_level = may
    ```

  - Force encryption

    ```
    smtpd_tls_security_level = encrypt
    ```

- Reload Postfix

MTA encryption(2-2) - Set up SMTP over TLS

❑ Now your server supports SMTP over TLS

```
 > telnet demo1.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to demo1.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
EHLO linuxhome.cs.nctu.edu.tw
250-demo1.nasa.lctseng.nctucs.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

❑ If you use force encryption, you must STARTTLS before sending mails

```
MAIL FROM: lctseng@nasa.lctseng.nctucs.net
530 5.7.0 Must issue a STARTTLS command first
```

MTA encryption(3-1)
- Set up SMTPs

- ❑ Alternative way to encrypt SMTP sessions
- ❑ Use different port: 465
- ❑ Force encryption
- ❑ Can coexist with SMTP over TLS
- ❑ In master.cf
  - Uncomment these lines

```
smtps     inet  n       -       n       -       -       smtpd
    -o syslog_name=postfix/smtps
    -o smtpd_tls_wrappermode=yes
```

  - This will open port 465 for SMTPs and use “smtps” as syslog name
- ❑ Reload Postfix

MTA encryption(3-2)
- Set up SMTPs

❑ Now you can use SSL clients to use SMTPs

- telnet may not work in encrypted sessions
- SSL client:

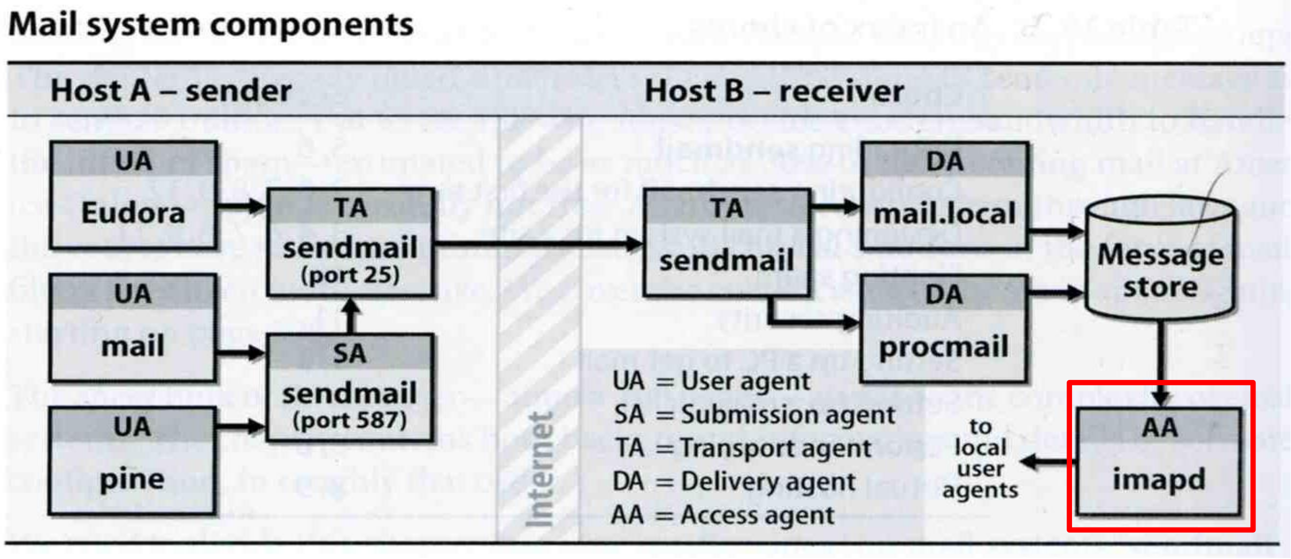
```
openssl s_client -connect host:port
```

- Important note
  - ➢ In openssl s_client, DO NOT use capital character “R”
    - – “R” is a special command in openssl s_client (for renegotiating)
  - ➢ So use “rcpt to” instead of “RCPT TO”
    - – For SMTP, they are all the same
  - ➢ If you use “R”, you will see following output (NOT a part of SMTP)

```
RENEGOTIATING
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X1
verify return:1
depth=0 CN = nasa.lctseng.nctucs.net
verify return:1
```

MAA for POP3 and IMAP

Read mails from remote host



MAA for POP3 and IMAP (1) - Read mails from terminal

- ❑ In fact, you mail server can receive mails now
  - But all messages are store in local disk
- ❑ To read mails, you must login via ssh
  - Built-in command to read mail: “mail”
  - Friendly command-line MUA: “mutt”
    - Packages:
      - zh-mutt (Chinese version)
      - mutt (English version)
    - Ports:
      - chinese/mutt
      - mail/mutt
- ❑ How to read mails from remote host?
  - MUA like Outlook, Thunderbird, or even Gmail
  - We need MAA

MAA for POP3 and IMAP (2)

- ❑ Fortunately, the Dovecot already provides POP3 and IMAP services
  - Include SSL versions: POP3s, IMAPs
    - ➢ That why we need SSL certificates and keys for Dovecot
- ❑ When you activate Dovecot service, these MAA services are also brought up.
- ❑ But you cannot access mail directly, you need some configuration
  - Configuration files are in : /usr/local/etc/dovecot/
  - There are many files included by dovecot.conf
    - ➢ In conf.d directory
    - ➢ Splitting configuration files is easier to management
  - Reference: http://wiki2.dovecot.org/QuickConfiguration

MAA for POP3 and IMAP (3) - Dovecot Configuration

❑ Allow GID = 0 to access mail (optional)

- By default, Dovecot do not allow users with GID = 0 to access mail. If your users are in wheel group, you need following settings
- In dovecot.conf

```
first_valid_gid = 0
```

❑ Specify the mail location

- In conf.d/10-mail.conf

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

❑ Add authenticate configuration to use PAM module

- Dovecot use system PAM module to authenticate
- Allow system users to access mails
- Create a new file: /etc/pam.d/dovecot

```
auth    required        pam_unix.so
account required        pam_unix.so
```

MAA for POP3 and IMAP (4)

- ❑ After restart Dovecot, your MAA is ready
- ❑ To check these services, you can use “telnet” or “openssl s_client”
  - POP3: 110
  - POP3s: 995
  - IMAP: 143
  - IMAPs: 993
- ❑ Messages for these services when you connect to the server
  - POP3

```
+OK Dovecot ready.
```

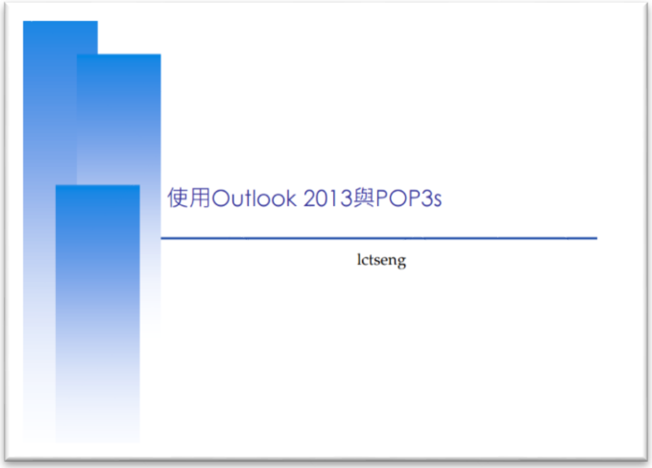
  - IMAP

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS
  ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

MAA for POP3 and IMAP (5)

❑ Set up MUAs like Outlook or Thunderbird

- You can see the tutorial in CS mail server, they should be similar to set up your server
- Settings for Gmail is also available
- https://mail.cs.nctu.edu.tw/


使用Outlook 2013與POP3s

lctseng

使用Gmail

lctseng

範例Gmail取樣日期：2014-10-31

Postfix Configuration

Reference: http://www.postfix.org/postconf.5.html

Postfix Configuration – Lookup tables (1)

- ❑ Parameters that use external files to store values
  - Such as mydestination, mynetwork, relay_domains
  - Text-based table is ok, but time-consuming when table is large
- ❑ Lookup tables syntax
  - Key   values
- ❑ postmap command
  - % postmap /etc/access   (generate database)
  - % postmap –q 140.113.235.150 /etc/access   (query)

```
140.113.235.150 REJECT
140.113.235     OK
```

/etc/access

```
> postmap -q 140.113.235.150 /etc/access
REJECT
> postmap -q 140.113.235 /etc/access
OK
```

Postfix Configuration – Lookup tables (2)

- ❑ Database format
  - % postconf –m
    - ➢ List all available database format
  - % postconf default_database_type
- ❑ Use databased-lookup table in main.cf
  - syntax

    Parameter = type:name

    or

    Parameter = option type:name

```
% postconf -m
btree
cidr
environ
hash
pcre
proxy
regexp
static
unix
% postconf default_database_type
default_database_type = hash
```

Postfix Configuration – Lookup tables (3)

❑ Example: Reject SMTP clients

- In main.cf

```
smtpd_client_restrictions =
        check_client_access hash:/etc/access
```

- Try SMTP clients from rejected host

```
rcpt to: lctseng@nasa.lctseng.nctucs.net
554 5.7.1 <linuxhome.cs.nctu.edu.tw[140.113.235.150]>:
         Client host rejected: Access denied
```

Postfix Configuration – Lookup tables (4)

❑ Regular expression tables

- More flexible for matching keys in lookup tables
- Two regular expression libraries used in Postfix
  - ➢ POSIX extended regular expression (regexp, default)
  - ➢ Perl-Compatible regular expression (PCRE)
- Usage
  - ➢ /pattern/ value
  - ➢ It is useful to use regular expression tables to do checks, such as
    - – header_checks parameters
    - – body_checks parameters

Postfix Configuration – system-wide aliases files

- ❑ Using aliases in Postfix
  - alias_maps = hash:/etc/aliases
  - alias_maps = hash:/etc/aliases, nis:mail.aliases
  - alias_database = hash:/etc/aliases
    - ➢ Tell newaliases command which aliases file to build
  - alias_maps: may not control by Postfix (may be NIS)
  - alias_database: under control by Postfix
- ❑ To Build alias database file
  - % postalias /etc/aliases
- ❑ Alias file format (same as sendmail)
  - RHS can be
    - ➢ Email address, filename, |command, :include:
- ❑ Alias restriction
  - allow_mail_to_commands = alias, forward
  - allow_mail_to_files = alias, forward

Postfix Configuration – MTA Identity

- Four related parameters
  - myhostname
    - myhostname = nabsd.cs.nctu.edu.tw
    - If un-specified, postfix will use ‵hostname′ command
  - mydomain
    - mydomain = cs.nctu.edu.tw
    - If un-specified, postfix use myhostname minus the first component
  - myorigin
    - myorigin = $mydomain (default is myhostname)
    - Used to append unqualified address
  - mydestination
    - List all the domains that postfix should accept for local delivery
    - mydestination = $myhostname, localhost.$mydomain $mydomain
      - This is the CS situation that mx will route mail to mailgate
    - mydestination = $myhostname, localhost.$mydomain

Postfix Configuration – Relay Control (1)

- Open relay
  - A mail server that permit anyone to relay mails
  - Often abused by spammer
    - Denied by other domains due to blacklist mechanism
  - By default, postfix is not an open relay

- A mail server should
  - Relay mail for trusted user
    - Such as smtp.cs.nctu.edu.tw trust all authenticated users
  - Relay mail for trusted domain
    - Such as smtp.csie.nctu.edu.tw trust nctu.edu.tw

Postfix Configuration – Relay Control (2)

- ❑ Restricting relay access by mynetworks_style
  - mynetworks_style = subnet
    - ➢ Allow relaying from other hosts in the same subnet
  - mynetworks_style = host
    - ➢ Allow relaying for only local machine
  - mynetworks_style = class
    - ➢ Any host in the same class A, B or C

- ❑ Restricting relay access by mynetworks
  - List individual IP or subnets in network/netmask notation
  - Ex: in /usr/local/etc/postfix/mynetworks
    - ➢ 127.0.0.0/8
    - ➢ 140.113.0.0/16
    - ➢ 10.113.0.0/16

- ❑ Relay depends on what kind of your mail server is
  - smtp.cs.nctu.edu.tw will be different from csmx1.cs.nctu.edu.tw

Postfix Configuration – master.cf (1)

❑ /usr/local/etc/postfix/master.cf

- Define what services the master daemon can invoke
- Each row defines a service and
- Each column contains a specific configuration option

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
flush     unix  n       -       n       1000?   0       flush
127.0.0.1:10025 inet    n       -       n       -       -       smtpd
```

Postfix Configuration – master.cf (2)

❑ Configuration options

- Service name and transport type
  - ➢ inet
    - – Network socket
    - – In this type, name can be combination of IP:Port
  - ➢ unix and fifo
    - – Unix domain socket and named pipe respectively
    - – Inter-process communication through file
- private
  - ➢ Access to this component is restricted to the Postfix system
- unpriv
  - ➢ Run with the least amount of privilege required
    - – y will run with the account defined in “mail_owner”
    - – n will run with root privilege

Postfix Configuration – master.cf (3)

- chroot
  - chroot location is defined in “queue_directory”
- wakeup
  - Periodic wake up to do jobs, such as pickup daemon
- maxproc
  - Number of processes that can be invoked simultaneously
  - Default count is defined in “default_process_limit”
  - 0: no limitation
- command + args
  - Default path is defined in “daemon_directory”
  - /usr/libexec/postfix

Postfix Configuration – Receiving limits

❑ Enforce limits on incoming mail

- The number of recipients for single delivery
  - ➢ smtpd_recipient_limit = 1000
- Message size
  - ➢ message_size_limit = 10240000
- The number of errors before breaking off communication
  - ➢ Postfix keep a counter of errors for each client and increase delay time once there is error
    - – E.g. No such user
  - ➢ smtpd_error_sleep_time = 1s
    - – Delay all responses if there are too many errors
    - – Between soft and hard limit
  - ➢ smtpd_soft_error_limit = 10
  - ➢ smtpd_hard_error_limit = 20
    - – Force disconnect if exceeds

Postfix Configuration – Rewriting address (1)

- For unqualified address
  - To append "myorigin" to local name.
    - append_at_myorigin = yes
  - To append "mydomain" to address that contain only host.
    - append_dot_mydomain = yes
- Masquerading hostname
  - Hide the names of internal hosts to make all addresses appear as if they come from the mail gateway
  - It is often used in out-going mail gateway
    - masquerade_domains = cs.nctu.edu.tw
    - masquerade_domains = !chairman.cs.nctu.edu.tw cs.nctu.edu.tw
    - masquerade_exceptions = admin, root
  - Rewrite to all envelope and header address excepts envelope recipient address
    - masquerade_class = envelope_sender, header_sender, header_recipient

Postfix Configuration – Rewriting address (2)

❑ Canonical address

- Rewrite both header and envelope recursively invoked by cleanup daemon
- Configuration
  - canonical_maps = hash:/usr/local/etc/postfix/canonical
  - canonical_classes = envelope_sender, envelope_recipient, header_sender, header_recipient
- /usr/local/etc/postfix/canonical

```
lctseng@cs.nctu.edu.tw        lctseng.NETADM@cs.nctu.edu.tw
lctseng@cs.nctu.edu.tw        lctseng@nabsd.cs.nctu.edu.tw
```

- Simlar maps
  - sender_canonical_maps
  - recipient_canonical_maps

Postfix Configuration – Rewriting address (3)

❑ Relocated users

- Used to inform sender that the recipient is moved
- relocated_maps = hash:/usr/local/etc/postfix/relocated
- Ex:

```
@nabsd.cs.nctu.edu.tw        nasa.cs.nctu.edu.tw
alice@nasa.cs.nctu.edu.tw    bob@abc.com
```

```
rcpt to: alice@nasa.lctseng.nctucs.net
550 5.1.6 <alice@nasa.lctseng.nctucs.net>:
   Recipient address rejected: User has moved to bob@abc.com
```

❑ Unknown users

- Not local user and not found in maps
- Default action: reject

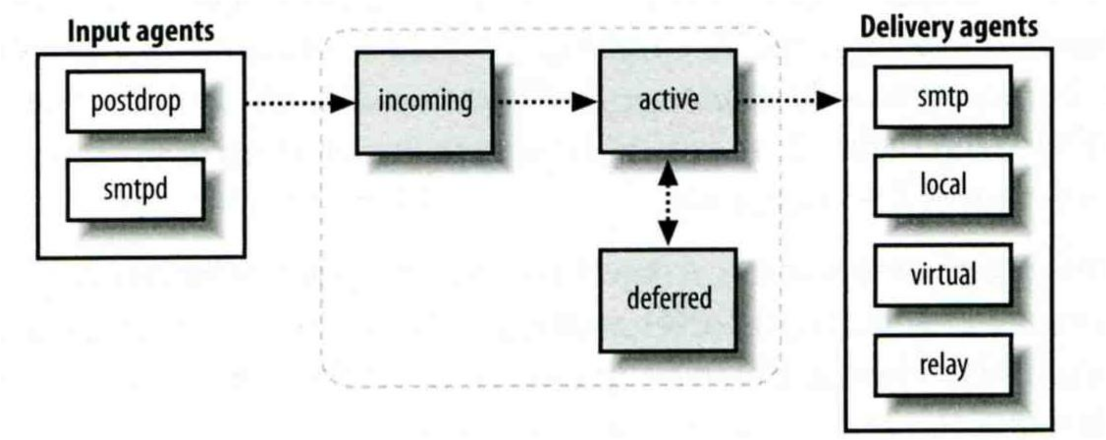
Queue Management

❑ The queue manage daemon

- qmgr daemon
- Queue directories (under /var/spool/postfix)
  - ➢ active, bounce, corrupt, deferred, hold

❑ Message movement between queues

- Temporary problem → deferred queue
- qmgr takes messages alternatively between incoming and deferred queue to active queue



Queue Management – Queue Scheduling

- ❑ Double delay in deferred messages
  - Between
    - ➢ minimal_backoff_time = 1000s
    - ➢ maximal_backoff_time = 4000s
  - qmgr daemon periodically scan deferred queue for reborn messages
    - ➢ queue_run_delay = 1000s
- ❑ Deferred → bounce
  - maximal_queue_lifetime = 5d
    - ➢ Exceeds → this messages is undeliverable
    - ➢ Set to 0: mail delivery should be tried only once

Queue Management – Message Delivery

- Controlling outgoing messages
  - When there are lots of messages in queue for the same destination, it should be careful not to overwhelm it
  - If concurrent delivery is success, postfix can increase concurrency between:
    - initial_destination_concurrency = 5
    - default_destination_concurrency_limit = 20
    - Under control by
      - maxproc in /usr/local/etc/postfix/master.cf
      - default_process_limit
    - You can override the default_destination_concurrency_limit for any transport mailer:
      - smtp_destination_concurrency_limit = 25
      - local_destination_concurrency_limit = 10
  - Control how many recipients for a single outgoing message
    - default_destination_recipient_limit = 50
    - You can override it for any transport mailer in the same idea:
      - smtp_destination_recipient_limit = 100

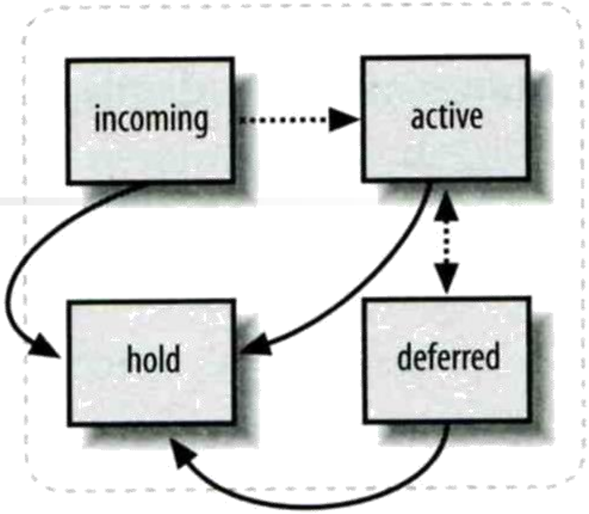
Queue Management – Error Notification

❑Sending error messages to administrator

- Set notify_classes parameter to list error classes that should be generated and sent to administrator
  - Ex: notify_classes = resource, software
- Error classes

Error Class	Description	Noticed Recipient (all default to postmaster)
bounce	Send headers of bounced mails	bounce_notice_recipient
2bounce	Send undeliverable bounced mails	2boucne_notice_recipient
delay	Send headers of delayed mails	delay_notice_recipient
policy	Send transcript when mail is reject due to anti-spam restrictions	error_notice_recipient
protocol	Send transcript that has SMTP error	error_notice_recipient
resource	Send notice because of resource pro.	error_notice_recipient
software	Send notice because of software pro.	error_notice_recipient

Queue Management – Queue Tools (1)



- ❑ postqueue command
  - postqueue –p
    - ➢ Generate sendmail mailq output
  - postqueue –f
    - ➢ Attempt to deliver all queued mail
  - postqueue –s cs.nctu.edu.tw
    - ➢ Schedule immediate delivery of all mail queued for site
- ❑ postsuper command
  - postsuper –d DBA3F1A9 (from incoming, active, deferred, hold)
  - postsuper –d ALL
    - ➢ Delete queued messages
  - postsuper –h DBA3F1A9 (from incoming, active, deferred)
  - postsuper –h ALL
    - ➢ Put messages "on hold" so that no attempt is made to deliver it
  - postsuper –H DBA3F1A9
  - postsuper –H ALL
    - ➢ Release messages in hold queue
  - postsuper –r DBA3F1A9
  - postsuper –r ALL
    - ➢ Requeue messages into maildrop queue

Queue Management – Queue Tools (2)

- ❑ postcat
  - Display the contents of a queue file

```
nabsd [/home/lctseng] -lctseng- sudo postqueue -p
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
DEC003B50E2      344 Tue May  8 19:58:37  lctseng@nabsd.cs.nctu.edu.tw
        (connect to chbsd.cs.nctu.edu.tw[140.113.17.212]: Connection refused)
                                         lctseng@chbsd.cs.nctu.edu.tw

-- 0 Kbytes in 1 Request.

nabsd [/home/lctseng] -lctseng- sudo postcat -q DEC003B50E2
*** ENVELOPE RECORDS deferred/D/DEC003B50E2 ***
message_size:            344             252               1              0            344
message_arrival_time: Tue May  8 19:58:37 2007
create_time: Tue May  8 19:58:37 2007
named_attribute: rewrite_context=local
sender_fullname: Tsung-Hsi Weng
sender: lctseng@nabsd.cs.nctu.edu.tw
original_recipient: lctseng@chbsd.cs.nctu.edu.tw
recipient: lctseng@chbsd.cs.nctu.edu.tw
*** MESSAGE CONTENTS deferred/D/DEC003B50E2 ***
Received: by nabsd.cs.nctu.edu.tw (Postfix, from userid 1001)
 id DEC003B50E2; Tue,  8 May 2007 19:58:37 +0800 (CST)
To: lctseng@chbsd.cs.nctu.edu.tw
Subject: Testing Mail
Message-Id: <20070508115837.DEC003B50E2@nabsd.cs.nctu.edu.tw>
Date: Tue,  8 May 2007 19:58:37 +0800 (CST)
From: lctseng@nabsd.cs.nctu.edu.tw (Liang-Chi Tseng)

hello
*** HEADER EXTRACTED deferred/D/DEC003B50E2 ***
*** MESSAGE FILE END deferred/D/DEC003B50E2 ***
```

Mail Relaying – Transport Maps (1)

- Transport maps
  - It override default transport types for delivery of messages
  - transport_maps = hash:/usr/local/etc/postfix/transport
  - Ex:

```
domain_or_address transport:nexthop
csie.nctu.edu.tw          smtp:[mailgate.csie.nctu.edu.tw]
cs.nctu.edu.tw            smtp:[csmailgate.cs.nctu.edu.tw]
cis.nctu.edu.tw           smtp:[mail.cis.nctu.edu.tw]

example.com               smtp:[192.168.23.56]:20025
orillynet.com             smtp
ora.com                   maildrop
kdent@ora.com             error:no mail accepted for kdent
```

Mail Relaying – Transport Maps (2)

- ❑ One usage in transport map
  - Postponing mail relay
    - ➢ Such as ISP has to postpone until customer network is online
  - Ex:

I am an ISP, and I has a mail server that is MX for abc.com

In /usr/local/etc/postfix/transport

```
abc.com      ondemand
```

In /usr/local/etc/postfix/master.cf

```
ondemand   unix   -   -   n   -   -   smtp
```

In /usr/local/etc/postfix/main.cf

```
defer_transports = ondemand
transport_maps = hash:/usr/local/etc/postfix/transport
```

No auto deliver for this transport name

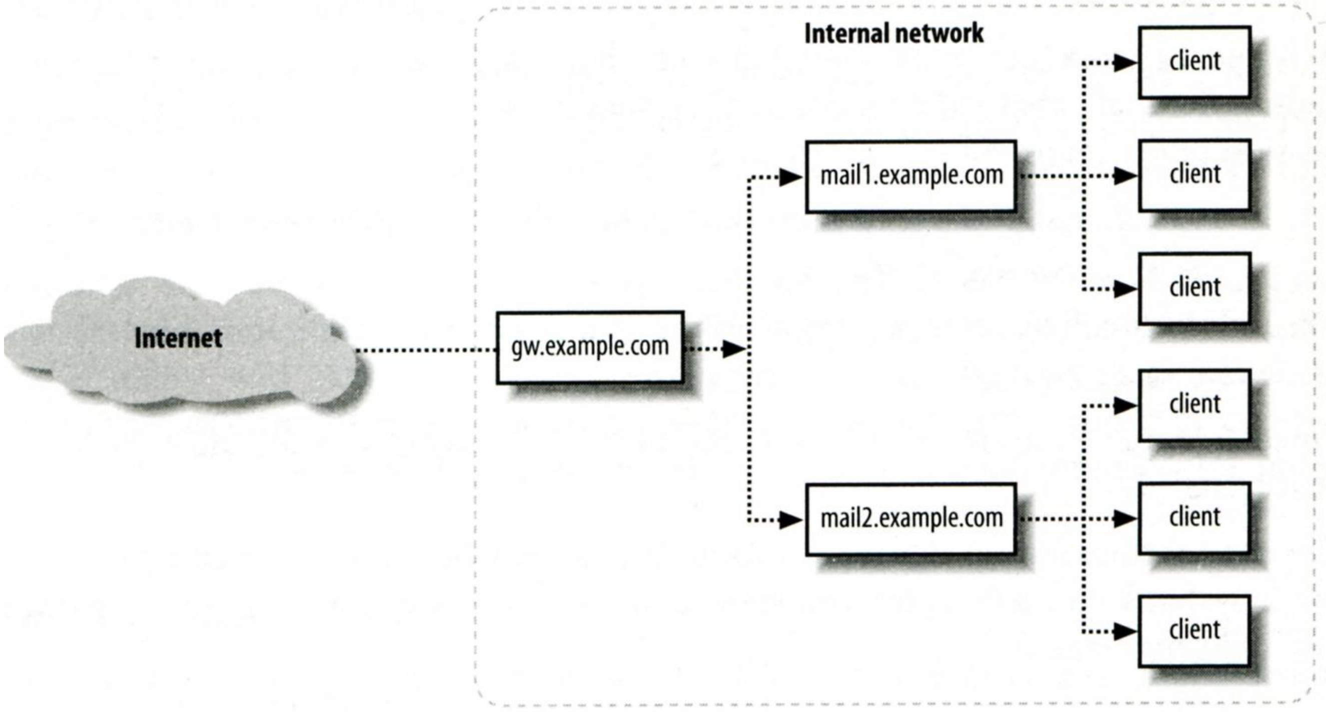
Whenever the customer network is online, do

```
$ postqueue –f abc.com
```

Mail Relaying – Inbound Mail Gateway (1)

❑ Inbound Mail Gateway

- Accept all mail for a network from the Internet and relays it to internal mail systems
- Ex:
  - csmx1.cs.nctu.edu.tw is a IMG
  - csmailgate.cs.nctu.edu.tw is internal mail system



Mail Relaying – Inbound Mail Gateway (2)

❑ To be IMG, suppose

- You are administrator for cs.nctu.edu.tw
- You have to be the IMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw

1. The MX record for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw should point to csmx1.cs.nctu.edu.tw
2. In csmx1.cs.nctu.edu.tw,

```
relay_domains = secureLab.cs.nctu.edu.tw javaLab.cs.nctu.edu.tw
transport_maps = hash:/usr/local/etc/postfix/transport
secureLab.cs.nctu.edu.tw        relay:[secureLab.cs.nctu.edu.tw]
javaLab.cs.nctu.edu.tw          relay:[javaLab.cs.nctu.edu.tw]
```

3. In secureLab.cs.nctu.edu.tw (and so do javaLab.cs.nctu.edu.tw)

```
mydestination = secureLab.cs.nctu.edu.tw
```

Mail Relaying – Outbound Mail Gateway

- ❑ Outbound Mail Gateway
  - Accept mails from inside network and relay them to Internet hosts on behalf of internal mail servers
- ❑ To be OMG, suppose
  - You are administrator for cs.nctu.edu.tw
  - You have to be the OMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw

1. In csmailer.cs.nctu.edu.tw

   mynetworks = hash:/usr/local/etc/postfix/mynetworks

   secureLab.cs.nctu.edu.tw

   javaLab.cs.nctu.edu.tw
2. All students in secureLab/javaLab will configure there MUA (ex. outlook) to use secureLab/javaLab.cs.nctu.edu.tw to be the SMTP server
3. In secureLab/javaLab.cs.nctu.edu.tw,

   relayhost = [csmailer.cs.nctu.edu.tw]

The next-hop destination of non-local mail

Advanced Aliasing – Virtual Alias Maps

❑ Virtual Alias Map

- It rewrites recipient addresses for all local, all virtual, and all remote mail destinations.
  - ➢ Route virtual email addresses to real users on the system
- virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
- Ex:

src-address	dst-address
lctseng@csie.nctu.edu.tw	@chbsd.cs.nctu.edu.tw
@csie.nctu.edu.tw	@cs.nctu.edu.tw
lctseng	lctseng@gmai1.com

- Applying regular expression
  - ➢ virtual_alias_maps = pcre:/usr/local/etc/postfix/virtual

```
/lctseng@csie\.nctu\.edu\.tw/          @chbsd.cs.nctu.edu.tw
/@csie\.nctu\.edu\.tw/                 @cs.nctu.edu.tw
/(\S+)\.(\S+)@cs\.nctu\.edu\.tw/       $1@cs.nctu.edu.tw
```

Multiple Domains

- ❑ Use single system to host many domains
  - Ex:
    - ➢ We use csmailgate.cs.nctu.edu.tw to host both
      - – cs.nctu.edu.tw
      - – csie.nctu.edu.tw
  - Purpose
    - ➢ Can be used for final delivery on the machine or
    - ➢ Can be used for forwarding to destination elsewhere
- ❑ Important considerations
  - Does the same user id with different domain should go to the same mailbox or different mailbox ?
    - ➢ YES (shared domain)
    - ➢ NO (Separate domain)
  - Does every user require a system account in /etc/passwd ?
    - ➢ YES (system account)
    - ➢ NO (virtual account)

Multiple Domains – Shared Domain with System Account

- ❑ Situation
  - The mail system should accept mails for both canonical and virtual domains and
  - The same mailbox for the same user id
- ❑ Procedure
  - Modify "mydomain" to canonical domain
  - Modify "mydestination" parameter to let mails to virtual domain can be local delivered
  - Ex:
    - ➢ mydomain = cs.nctu.edu.tw
    - ➢ mydestination = $myhostname, $mydomain, csie.nctu.edu.tw

    ※ In this way, mail to both lctseng@cs.nctu.edu.tw and lctseng@csie.nctu.edu.tw will go to csmailgate:/var/mail/lctseng
- ❑ Limitation
  - Can not separate lctseng@cs.nctu.edu.tw from lctseng@csie.nctu.edu.tw

Multiple Domains – Separate Domains with System Accounts

- ❑ Situation
  - The mail system should accept mails for both canonical and virtual domains and
  - Mailboxes are not necessarily the same for the same user id
- ❑ Procedure
  - Modify "mydomain" to canonical domain
  - Modify "virtual_alias_domains" to accept mails to virtual domains
  - Create "virtual_alias_maps" map
  - Ex:
    - ➢ mydomain = cs.nctu.edu.tw
    - ➢ virtual_alias_domains = abc.com.tw, xyz.com.tw
    - ➢ virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
    - ➢ In /usr/local/etc/postfix/virtual

```
– CEO@abc.com.tw          andy
– @xyz.com.tw             jack
```

- ❑ Limitation
  - Need to maintain UNIX account for virtual domain user

Multiple Domains –

Separate Domains with Virtual Accounts (1)

❑ Useful when users in virtual domains:

- Do not need to login to system
- Only need to retrieve mail through POP/IMAP server

❑ Procedure

- Modify “virtual_mailbox_domains” to let postfix know what mails it should accepts
  - ➢ Or simply included in “virtual_mailbox_maps” map
- Modify “virtual_mailbox_base” and create related directory to put mails
- Create “virtual_mailbox_maps” map
- Ex:
  - ➢ Create /var/vmail/abc-domain and /var/vmail/xyz-domain

```
virtual_mailbox_base = /var/vmail
virtual_mailbox_maps = hash:/usr/local/etc/postfix/vmailbox
```

  - ➢ In /usr/local/etc/postfix/vmailbox

```
abc.com.tw       this-text-is-ignore
xyz.com.tw       this-text-is-ignore
CEO@abc.com.tw    abc-domain/CEO
CEO@xyz.com.tw    xyz-domain/CEO/
```

MailBox format

MailDir format

Multiple Domains – Separate Domains with Virtual Accounts (2)

- ❑ Ownerships of virtual mailboxes
  - Simplest way:
    - ➢ The same owner of POP/IMAP Servers
  - Flexibility in postfix
    - ➢ virtual_uid_maps and virtual_gid_maps
    - ➢ Ex:
      - – virtual_uid_maps = static:143
      - – virtual_gid_maps = static:6
      - – virtual_uid_maps = hash:/usr/local/etc/postfix/virtual_uids
      - – virtual_uid_maps = hash:/usr/local/etc/postfix/virtual_uids static:143
      - – In /usr/local/etc/postfix/virtual_uids

```
» CEO@abc.com.tw        1004
» CEO@xyz.com.tw        1008
```

  - How to let virtual users authenticate and retrieve their mails?
    - ➢ You need other mechanism or modules (out of scope now)

Handling Spam in Postfix

Nature of Spam

- Spam – **S**imultaneously **P**osted **A**dvertising **M**essage
  - UBE – Unsolicited Bulk Email
  - UCE – Unsolicited Commercial Email
- Spam
  - There is no relationship between receiver and
    - Sender
    - Message content
  - Opt out instruction
  - Conceal trail
    - False return address
    - Forged header information
  - Use misconfigured mail system to be an accomplice
  - Circumvent spam filters either encode message or insert random letters

Problems of Spam

- ❑ Cost
  - Waste bandwidth and disk space
  - DoS like side-effect
  - Waste time and false deletion
  - Bounce messages of nonexistent users
    - ➢ Nonexistent return address
    - ➢ Forged victim return address
- ❑ Detection
  - Aggressive spam policy may cause high false positive

Anti-Spam – Client-Based Detection (1)

- ❑ Client-blocking
  - Use IP address, hostnames or email address supplied by clients when they connect to send a message
  - Compared with Spammer list
  - Problems
    - ➢ IP address, hostname, email address are forged
    - ➢ Innocent victim open relay host
- ❑ DNSBL (DNS-based Blacklist)
  - Maintain large database of systems that are known to be open relays or that have been used for spam
- ❑ Grey Listing
- ❑ SPF – Sender Policy Framework
- ❑ …

Anti-Spam – Client-Based Detection (2)

- What DNSBL maintainers do
  - Suppose csie has a Blacklist DNS database
    - Suppose DNSBL Domain "dnsbl.cs.nctu.edu.tw"
  - If 140.112.23.118 is detected as open relay
    - There will be a new entry in cs's blacklist DB
      - 118.23.112.140.dnsbl.cs.nctu.edu.tw
  - When we receive a connection from 140.112.23.118
    - Compose 118.23.112.140.dnsbl.cs.nctu.edu.tw
    - DNS query for this hostname
      - Successful means this IP address is suspicious
      - Failed means ok
- Using DNSBL
  - Review their service options and policies carefully

Anti-Spam – Content-Based Detection

- ❑ Spam patterns in message body
- ❑ Detection difficulties
  - Embed HTML codes within words of their message to break up phrases
  - Randomly inserted words
  - Content-based detection is slower

Anti-Spam – Action

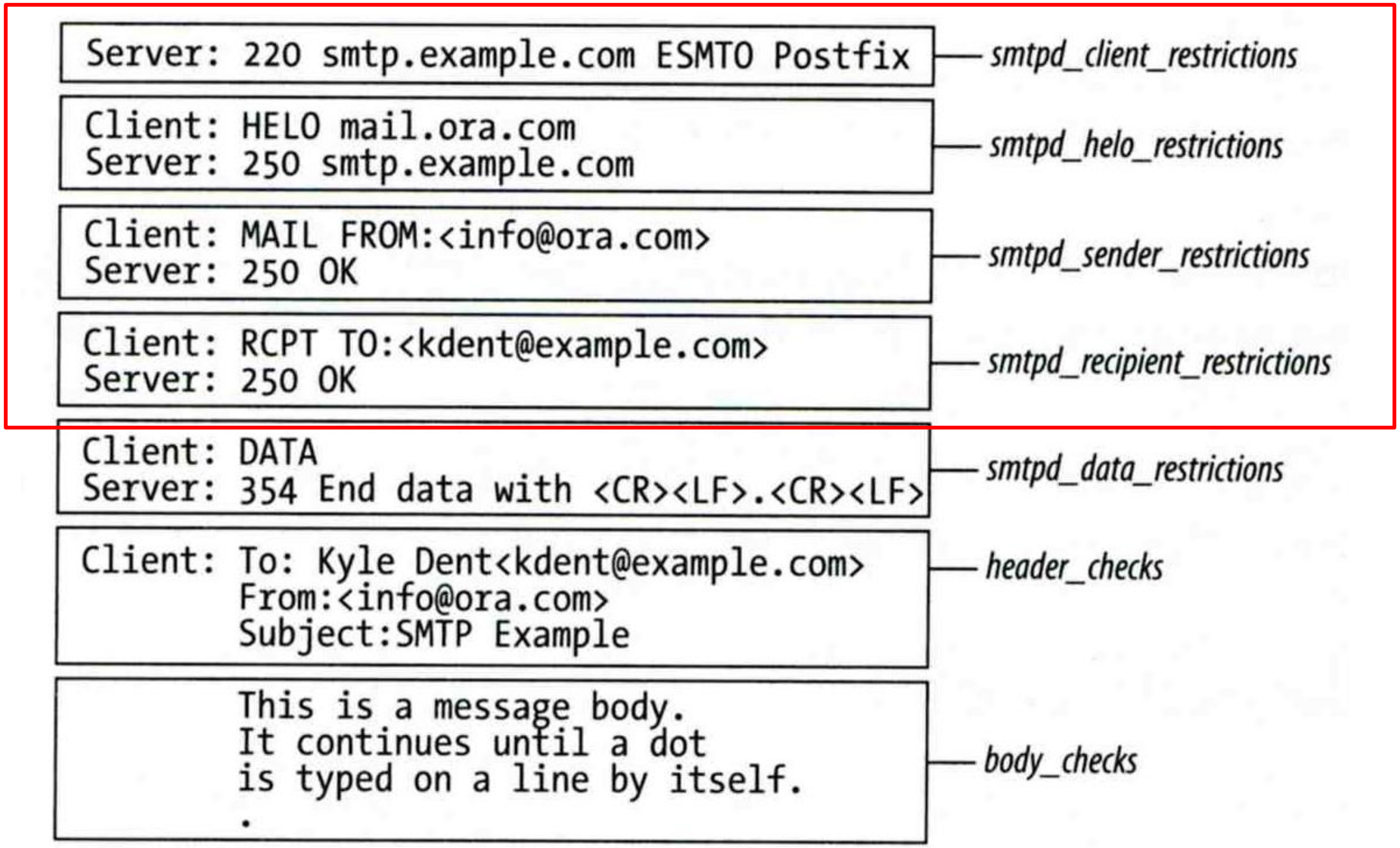
❑ When you detect a spam, you can:

- Reject immediately during the SMTP conversation
- Save spam into a suspected spam repository
- Label spam and deliver it with some kind of spam tag
- Ex:
  - X-Spam-Status: Yes, hits=18.694 tagged_above=3 required=6.3
  - X-Spam-Level: ******************
  - X-Spam-Flag: YES

Postfix Anti-Spam configuration

❑ The SMTP Conversation

- info@ora.com → smtp.example.com → kdent@example.com



```
Server: 220 smtp.example.com ESMTO Postfix

Client: HELO mail.ora.com
Server: 250 smtp.example.com

Client: MAIL FROM:<info@ora.com>
Server: 250 OK

Client: RCPT TO:<kdent@example.com>
Server: 250 OK

Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>

Client: To: Kyle Dent<kdent@example.com>
        From:<info@ora.com>
        Subject:SMTP Example

        This is a message body.
        It continues until a dot
        is typed on a line by itself.
        .
```

smtpd_client_restrictions
smtpd_helo_restrictions
smtpd_sender_restrictions
smtpd_recipient_restrictions
smtpd_data_restrictions
header_checks
body_checks

Postfix Anti-Spam configuration – Client Detection Rules (1)

- Four rules in relative detection position
  - Rules and their default values
    - smtpd_client_restrictions =
    - smtpd_helo_restrictions =
    - smtpd_sender_restrictions =
    - smtpd_recipient_restrictions =

      permit_mynetworks, reject_unauth_destination
  - Each restriction check result can be:
    - OK (Accept in this restriction)
    - REJECT (Reject immediately without further check)
    - DUNNO (do next check)
  - There are 5 types of restrictions

Postfix Anti-Spam configuration – Client Detection Rules (2)

1. Access maps
   - List of IP addresses, hostnames, email addresses
   - Can be used in:

```
smtpd_client_restrictions = check_client_access hash:/etc/access
smtpd_helo_restrictions = check_helo access hash:/usr/local/etc/postfix/helohost
smtpd_sender_restrictions = check_sender_access hash:/usr/local/etc/postfix/sender_access
smtpd_recipient_restrictions = check_recipient_access hash:/usr/local/etc/postfix/recipient_access
```

   - Actions
     - OK, REJECT, DUNNO
     - FILTER (redirect to content filter)
     - HOLD (put in hold queue)
     - DISCARD (report success to client but drop)
     - 4xx message or 5xx message

Postfix Anti-Spam configuration – Client Detection Rules (3)

- Example of access maps
  - check_client_access hash:/etc/access

```
nctu.edu.tw          OK
127.0.0.1            OK
61.30.6.207          REJECT
```

  - check_helo access hash:/postfix/helohost

```
greatdeals.example.com        REJECT
oreillynet.com                OK
```

  - check_sender_access hash:/usr/local/etc/postfix/sender_access

```
viagra.com           553 Please contact +886-3-5712121-54707.
aaa@                 553 Invalid MAIL FROM
sales@               553 Invalid MAIL FROM
hchen@               553 Invalid MAIL FROM
```

  - check_recipient_access hash:/usr/local/etc/postfix/recipient_access

```
bin@cs.nctu.edu.tw   553 Invalid RCPT TO command
ftp@cs.nctu.edu.tw   553 Invalid RCPT TO command
man@cs.nctu.edu.tw   553 Invalid RCPT TO command
```

Postfix Anti-Spam configuration – Client Detection Rules (4)

2. Special client-checking restrictions
   - permit_auth_destination
     - Mostly used in "smtpd_recipient_restrictions"
     - Permit request if destination address matches:
       - The postfix system's final destination setting
         - mydestination, inet_interfaces, vitual_alias_maps, virtual_mailbox_maps
       - The postfix system's relay domain
         - relay_domains
     - Found ➔ OK, UnFound ➔ DUNNO
   - reject_unauth_destination
     - Opposite to permit_auth_destination
     - Found ➔ REJECT, UnFound ➔ DUNNO
   - permit_mynetworks
     - Allow a request if interest IP match any address in "mynetworks"
       - Used in smtpd_recipient_restrictions
       - Used in smtpd_client_restrictions

Postfix Anti-Spam configuration – Client Detection Rules (5)

3. Strict syntax restrictions
   > Restrictions that does not conform to RFC

- reject_invalid_hostname
  - Reject hostname with bad syntax
- reject_non_fqdn_hostname
  - Reject hostname not in FQDN format (HELO or EHLO)
- reject_non_fqdn_sender
- reject_non_fqdn_recipient
  - For "MAIL FROM" and "RCPT TO" command respectively

Postfix Anti-Spam configuration – Client Detection Rules (6)

4. DNS restrictions
   - Make sure that clients and email envelope addresses have valid DNS information
   - reject_unknown_client
     - Reject if the client IP has no DNS PTR record
       - 215.17.113.140 IN PTR nabsd.cs.nctu.edu.tw.
     - False detection: many normal MTAs have A records only
   - reject_unknown_hostname
     - Reject if EHLO hostname has no DNS MX or A record
   - reject_unknown_sender_domain
     - Reject if MAIL FROM domain name has no DNS MX or A record
     - Spammers don’t want to receive return mails
   - reject_unknown_recipient_domain
     - Reject if RCPT TO domain name has no DNS MX or A record

Postfix Anti-Spam configuration – Client Detection Rules (7)

5. Real-time blacklists
   - Check with DNSBL services
   - reject_rbl_client domain.tld
     - Reject if client IP is detect in DNSBL
   - reject_rhsbl_client domain.tld
     - Reject if client hostname has an A record under specified domain
   - reject_rhsbl_sender domain.tld
     - Reject if MAIL FROM domain in address has an A record under specified domain
   - smtpd_client_restrictions =

     hash:/etc/access, reject_rbl_client relays.ordb.org
   - smtpd_sender_restrictions =

     hash:/usr/local/etc/postfix/sender_access, reject_rhsbl_sender dns.rfc-ignorant.org

Postfix Anti-Spam configuration – Client Detection Rules (8)

6. Policy Service
   - Postfix SMTP server sends in a delegated SMTPD access policy request to one special service (policy serivce).
   - Policy service replies actions allowed in Postfix SMTPD access table.
   - Usage:
     - check_policy_service *servicename*
   - Example: Grey Listing (Using Postgrey)
     - Postgrey daemon runs on port:10023
     - Don’t need to specify it in master.cf
     - In main.cf:

```
smtpd_recipient_restrictions = check_policy_service inet:127.0.0.1:10023
```

Postfix Anti-Spam configuration – Client Detection Rules (8)

❑smtpd_client_restrictions

- check_client_access
- reject_unknown_client
- permit_mynetworks
- reject_rbl_client
- reject_rhsbl_client

❑smtpd_helo_restrictions

- check_helo_access
- reject_invalid_hostname
- reject_unknown_hostname
- reject_non_fqdn_hostname

❑smtpd_sender_restrictions

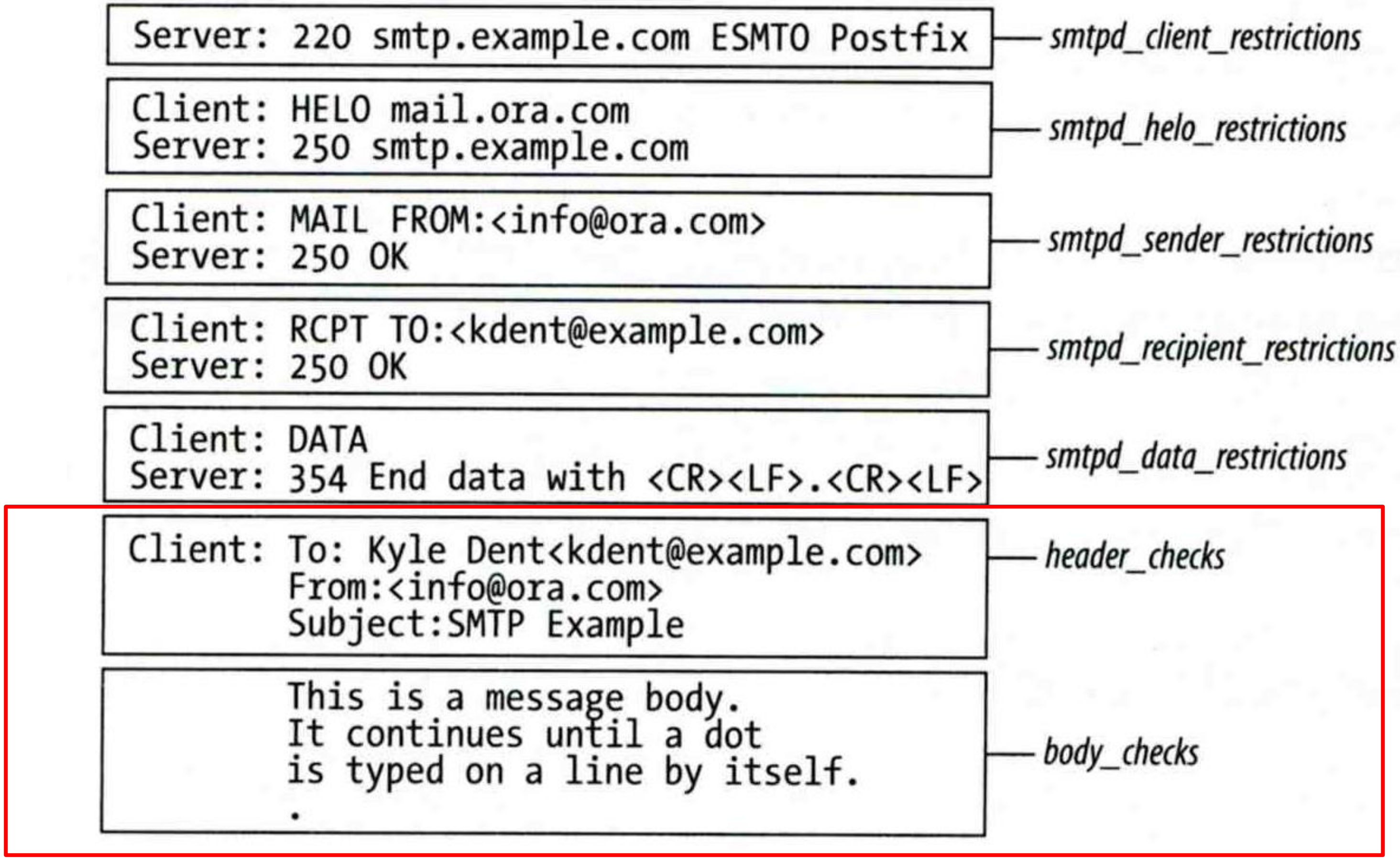
- check_sender_access
- reject_unknown_sender_domain
- reject_rhsbl_sender

❑smtpd_recipient_restrictions

- check_recipient_access
- permit_auth_destination
- reject_unauth_destination
- reject_unknown_recipient_domain
- reject_non_fqdn_recipient
- check_policy_service

Postfix Anti-Spam configuration

- ❑ The SMTP Conversation
  - info@ora.com → smtp.example.com → kdent@example.com



```
Server: 220 smtp.example.com ESMTO Postfix

Client: HELO mail.ora.com
Server: 250 smtp.example.com

Client: MAIL FROM:<info@ora.com>
Server: 250 OK

Client: RCPT TO:<kdent@example.com>
Server: 250 OK

Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>

Client: To: Kyle Dent<kdent@example.com>
        From:<info@ora.com>
        Subject:SMTP Example

        This is a message body.
        It continues until a dot
        is typed on a line by itself.
        .
```

smtpd_client_restrictions
smtpd_helo_restrictions
smtpd_sender_restrictions
smtpd_recipient_restrictions
smtpd_data_restrictions
header_checks
body_checks

Postfix Anti-Spam configuration – Content-Checking rules (1)

- ❑ 4 rules
  - header_checks
    - ➢ Check for message headers
  - mime_header_checks
    - ➢ Check for MIME headers
  - nested_header_checks
    - ➢ Check for attached message headers
  - body_check
    - ➢ Check for message body
- ❑ All rules use lookup tables
  - Ex:

```
header_checks = regexp:/usr/local/etc/postfix/header_checks
body_checks = pcre:/usr/local/etc/postfix/body_checks
```

Postfix Anti-Spam configuration – Content-Checking rules (2)

- ❑ Content-checking lookup table
  - Regular_Expression   Action
- ❑ Actions
  - REJECT message
  - WARN message
    - ➢ Logs a rejection without actually rejecting
  - IGNORE
    - ➢ Delete matched line of headers or body
  - HOLD message
  - DISCARD message
    - ➢ Claim successful delivery but silently discard
  - FILTER message
    - ➢ Send message through a separate content filter (may be external program)

Postfix Anti-Spam configuration – Content-Checking rules (3)

- ❑ Example of header check
  - header_checks = regexp:/usr/local/etc/postfix/header_checks
  - In /usr/local/etc/postfix/header_checks

```
/take advantage now/               REJECT
/repair your credit/               REJECT
```

- ❑ Example of body check
  - body_checks = regexp:/usr/local/etc/postfix/body_checks
  - In /usr/local/etc/postfix/body_checks

```
/lowest rates.*\!/                 REJECT
/[:alpha:]<!--.*-->[:alpha:]/      REJECT
```

External Filters

- ❑ Filtering can be done on
  - MTA
  - MDA
  - MUA
  - ※ Combination of MTA and MUA
    - ➢ Adding some extra headers or modifying subject in MTA, and filtering in MUA.

- ❑ External filters for postfix
  - Command-based filtering
    - ➢ New process is started for every message
    - ➢ Accept message from STDIN
  - Daemon-based filtering
    - ➢ Stay resident
    - ➢ Accept message via SMTP or LMTP

MDA Filter: Procmail (1)

- Install procmail (port or package)
- Enable Procmail in Postfix
  - In main.cf

```
mailbox_command = /usr/local/bin/procmail
```

- Create configuration file
  - Create /usr/local/etc/procmailrc
- Create log files
  - touch /var/log/procmail.log
- Create directories (optional)
  - mkdir -p /tmp/trash

```
VERBOSE=off
LOGFILE=/var/log/procmail.log

:0b
* ^Subject:.*GGWP.*
/dev/null

:0b
* ^Subject:.*LOL.*
/tmp/trash
```

procmailrc

MDA Filter: Procmail (2-1) - Filter Chinese Text

- ❑ Encoding problem
  - We need to set two types of encoded Chinese text
  - Base64 and Quote-Printable
- ❑ Tool: mmencode (port or package)
- ❑ Generate encoded text
  - Filter “減肥”
  - Generate Base64 code

```
> echo -n "減肥" | mmencode
5rib6IKl
```

  - Generate QP code

```
> echo -n "減肥" | mmencode -q
=E6=B8=9B=E8=82=A5=
```

MDA Filter: Procmail (2-2) - Filter Chinese Text

- ❑ Write two rules to filter Chinese text

```
# Base64
:0b
* ^Subject:.*5rib6IKl.*
/dev/null

# Quote-Printable
:0b
* ^Subject:.*=E6=B8=9B=E8=82=A5=.*
/dev/null
```

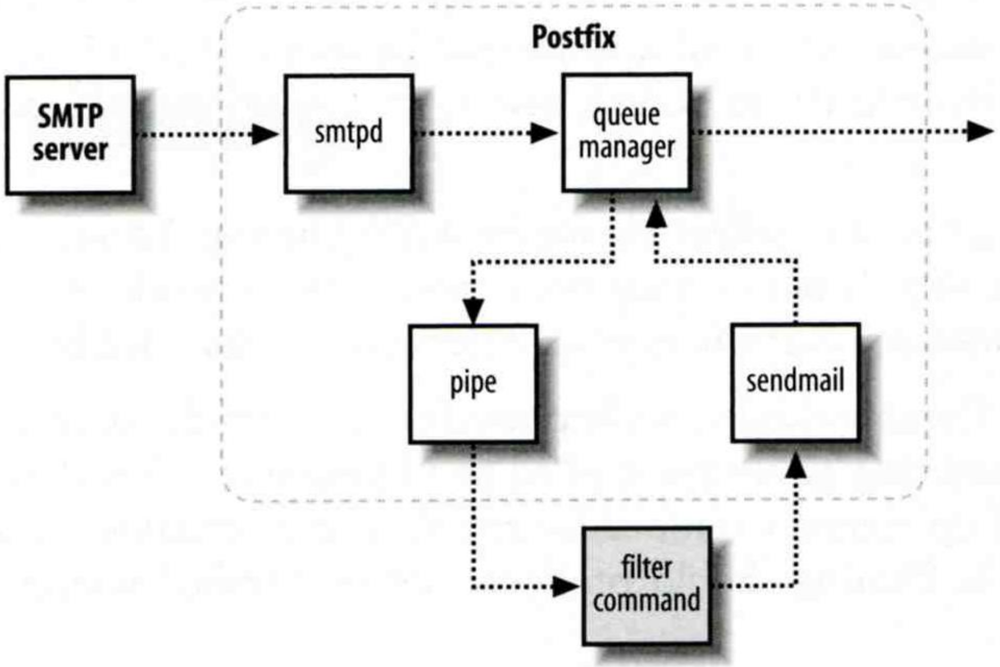
- ❑ Log file

```
From lctseng@nasa.lctseng.nctucs.net  Wed Mar  9 12:14:46 2016
 Subject: =?UTF-8?B?5rib6IKl?=
  Folder: /dev/null                                         1
```

Command-Based Filtering (1)

❑ Usage

- Postfix delivers message to this filter via “pipe” mailer
- Program that accepts content on its STDIN
- Program gives the filtered message back to Postfix using the “sendmail” command (with same queue ID)



Command-Based Filtering (2)

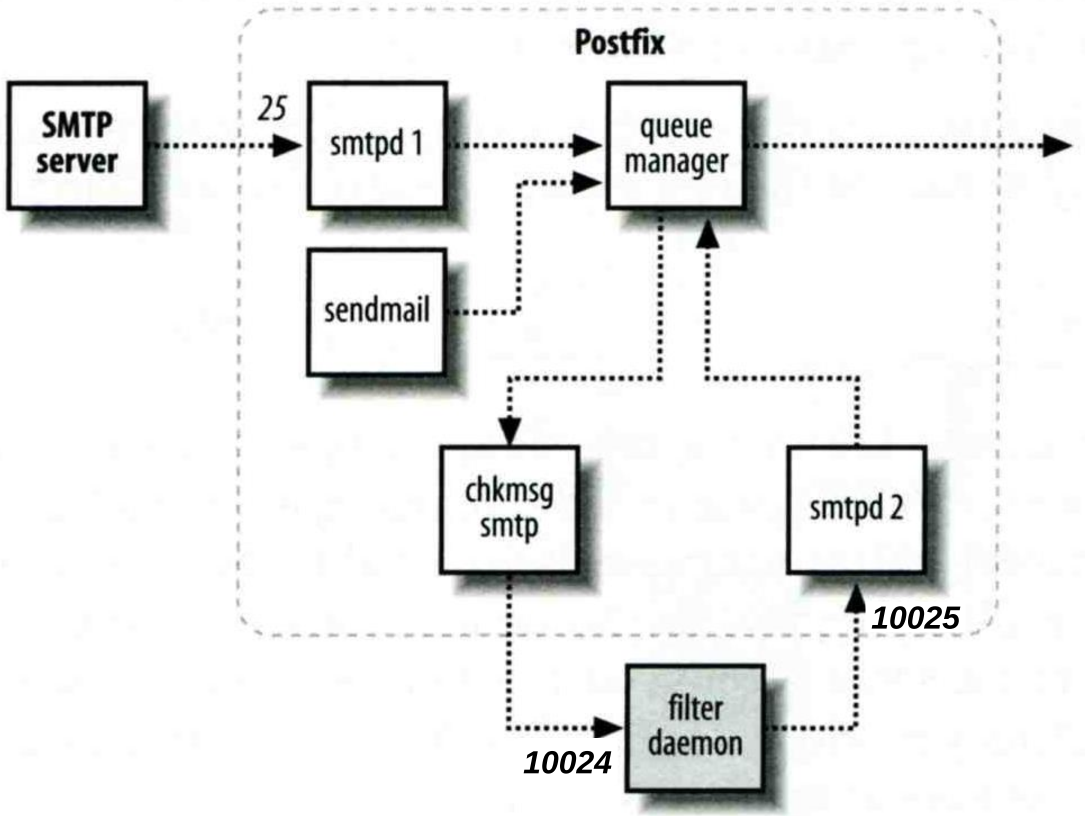
❑ Configuration

- Prepare your filter program (/usr/local/bin/simple_filt)
- Modify master.cf

```
#================================================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#================================================================================================
filter  unix  -   n        n      -       -       pipe
                  flags=Rq user=filter argv=/usr/local/bin/simple_filt -f ${sender} - -${recipient}
smtpd    inet  n       -        n      -       -       smtpd
                  -o content_filter=filter:
```

Daemon-Based Filtering (1)

- ❑ Usage
  - Message is passed back and forth between Postfix and filtering daemon via SMTP or LMTP



Daemon-Based Filtering (2) - amavisd-new

- ❑ Primary daemon: amavisd-new
  - Cooperate with other programs
  - Clamav (anti-virus), SpamAssassin (anti-spam)
- ❑ Configuration for amavisd
  - Install and configure your content filter
    - ➢ security/amavisd-new (port or package)
    - ➢ Modify amavisd.conf to send message back

```
$forward_method = 'smtp:127.0.0.1:10025';
```

  - Edit /etc/rc.conf

```
amavisd_enable="YES"
```

  - Edit main.cf to let postfix use filtering daemon

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Daemon-Based Filtering (3) - amavisd-new

- ❑ Configuration
  - Edit master.cf to add two additional services

```
smtp-amavis unix -      -       n       -       10       smtp
    -o smtp_data_done_timeout=1200s
    -o smtp_never_send_ehlo=yes
    -o notify_classes=protocol,resource,software
127.0.0.1:10025 inet n  -       n       -       -       smtpd
    -o content_filter=
    -o mynetworks=127.0.0.0/8
    -o local_recipient_maps=
    -o notify_classes=protocol,resource,software
    -o myhostname=localhost
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_tls_security_level=
```

Daemon-Based Filtering (4)
- amavisd-new

❑ Now, your amavisd-new is ready

- With SpamAssassin installed
- Run “sa-update” to update the SpamAssassin rules
- Edit SpamAssassin configuration in amavisd.conf
    - ➢ E.g. Change spam detect level

```
$sa_tag2_level_deflt = 3.0;
```

Daemon-Based Filtering (5) - amavisd-new

❑ The mail source in SPAM-detected mail

```
Received: from demo1.nasa.lctseng.nctucs.net (localhost [127.0.0.1])
         by localhost (Postfix) with ESMTP id 1A945274
         for <lctseng@nasa.lctseng.nctucs.net>; Wed,  9 Mar 2016 14:14:39
+0800 (CST)
X-Virus-Scanned: amavisd-new at nasa.lctseng.ncatucs.net
X-Spam-Flag: YES
X-Spam-Score: 4.85
X-Spam-Level: ****
X-Spam-Status: Yes, score=4.85 tagged_above=2 required=3
         tests=[FREEMAIL_ENVFROM_END_DIGIT=0.25, FREEMAIL_FROM=0.001,
         HTML_FONT_LOW_CONTRAST=0.001, HTML_MESSAGE=0.001,
         RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H3=-0.01,
         RCVD_IN_MSPIKE_WL=-0.01, T_REMOTE_IMAGE=0.01,
URIBL_ABUSE_SURBL=1.948,
         URIBL_BLACK=1.7, URIBL_WS_SURBL=1.659] autolearn=no
autolearn_force=no
Authentication-Results: demo1.nasa.lctseng.nctucs.net (amavisd-new);
         dkim=pass (2048-bit key) header.d=gmail.com
Received: from demo1.nasa.lctseng.nctucs.net ([127.0.0.1])
         by demo1.nasa.lctseng.nctucs.net (demo1.nasa.lctseng.nctucs.net
[127.0.0.1]) (amavisd-new, port 10024)
         with SMTP id CjRyliYl5l6x for <lctseng@nasa.lctseng.nctucs.net>;
         Wed,  9 Mar 2016 14:14:38 +0800 (CST)
```

Daemon-Based Filtering (6) - amavisd-new + ClamAV

- ❑ amavisd-new supports lots of anti-virus scanner
- ❑ Anti-virus with ClamAV
  - Install security/clamav (port or package)
  - Edit /etc/rc.conf

```
clamav_clamd_enable="YES"
```

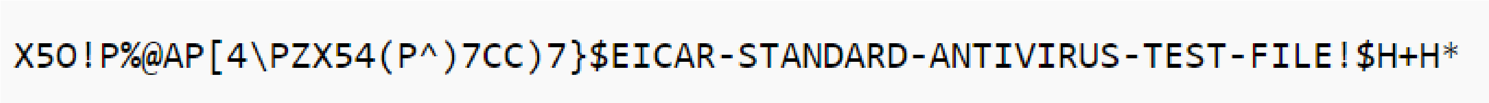
  - Update virus database
    - ➢ Run “freshclam”
  - Specify to use clamav in amavisd.conf

```
@av_scanners = (

['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
);
```

Daemon-Based Filtering (7) - amavisd-new + ClamAV

- ❑ Set alias for “virusalert” user
  - When there is an infected mail, it will send a notification to this user
  - Alias to “root” or “postmaster”
- ❑ Start ClamAV and restart amavisd-new
  - service clamav-clamd start
  - service amavisd restart
- ❑ Send a test virus by EICAR organization
  - Plain text

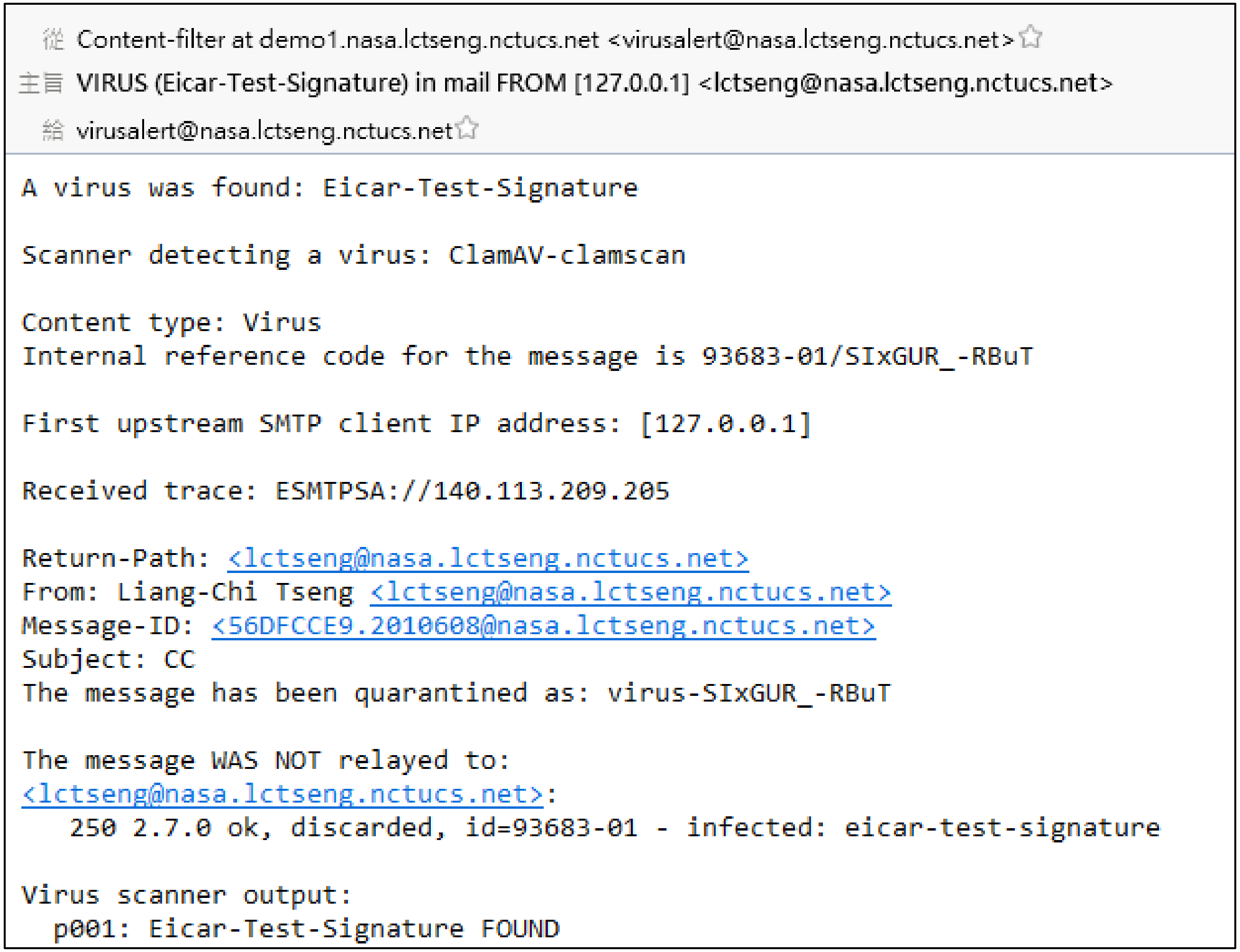


```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

  - Reference: https://en.wikipedia.org/wiki/EICAR_test_file

Daemon-Based Filtering (8) - amavisd-new + ClamAV

❑ Result of sending EICAR test mail



從 Content-filter at demo1.nasa.lctseng.nctucs.net <virusalert@nasa.lctseng.nctucs.net>

主旨 VIRUS (Eicar-Test-Signature) in mail FROM [127.0.0.1] <lctseng@nasa.lctseng.nctucs.net>

給 virusalert@nasa.lctseng.nctucs.net

```
A virus was found: Eicar-Test-Signature

Scanner detecting a virus: ClamAV-clamscan

Content type: Virus
Internal reference code for the message is 93683-01/SIxGUR_-RBuT

First upstream SMTP client IP address: [127.0.0.1]

Received trace: ESMTPSA://140.113.209.205

Return-Path: <lctseng@nasa.lctseng.nctucs.net>
From: Liang-Chi Tseng <lctseng@nasa.lctseng.nctucs.net>
Message-ID: <56DFCCE9.2010608@nasa.lctseng.nctucs.net>
Subject: CC
The message has been quarantined as: virus-SIxGUR_-RBuT

The message WAS NOT relayed to:
<lctseng@nasa.lctseng.nctucs.net>:
   250 2.7.0 ok, discarded, id=93683-01 - infected: eicar-test-signature

Virus scanner output:
  p001: Eicar-Test-Signature FOUND
```