Postfix

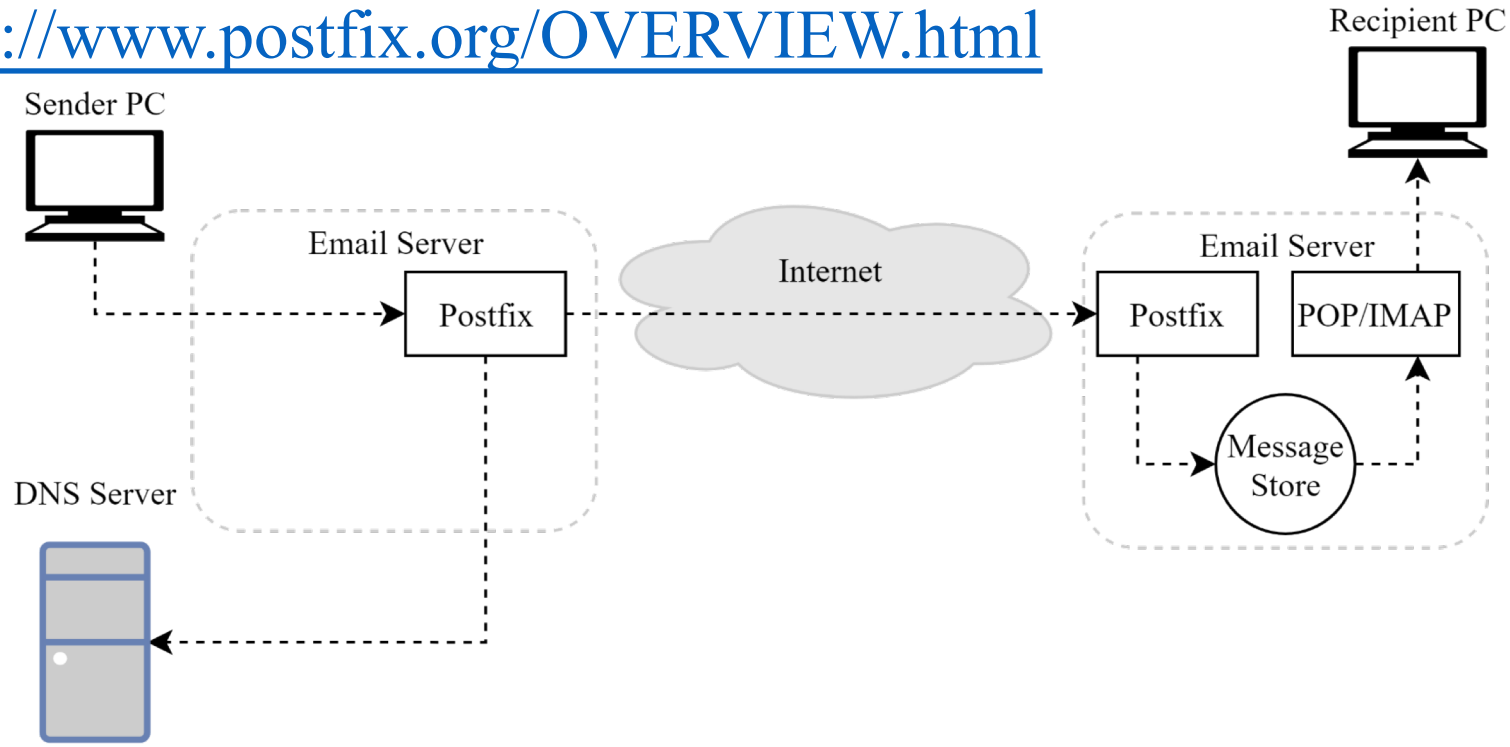
lctseng (2020-2022, CC-BY)
? (?-2019)
國立陽明交通大學資工系資訊中心
Computer Center of Department of Computer Science, NYCU

Postfix

- Postfix v3.6.x
  - Latest stable release: 3.7.0 (Feb 2022)
  - /usr/ports/mail/postfix
  - pkg install postifx
- http://www.postfix.org
  - http://www.postfix.org/documentation.html

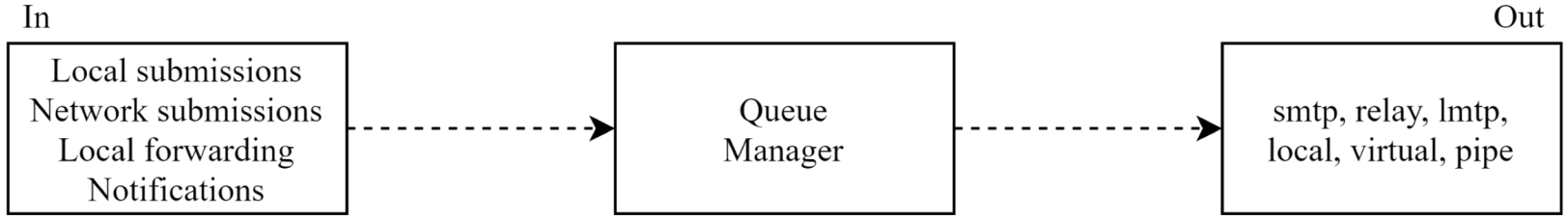
Role of Postfix

- MTA that
  - Receive and deliver email over the network via SMTP
  - Local delivery directly or use other mail delivery agent
    - http://www.postfix.org/OVERVIEW.html



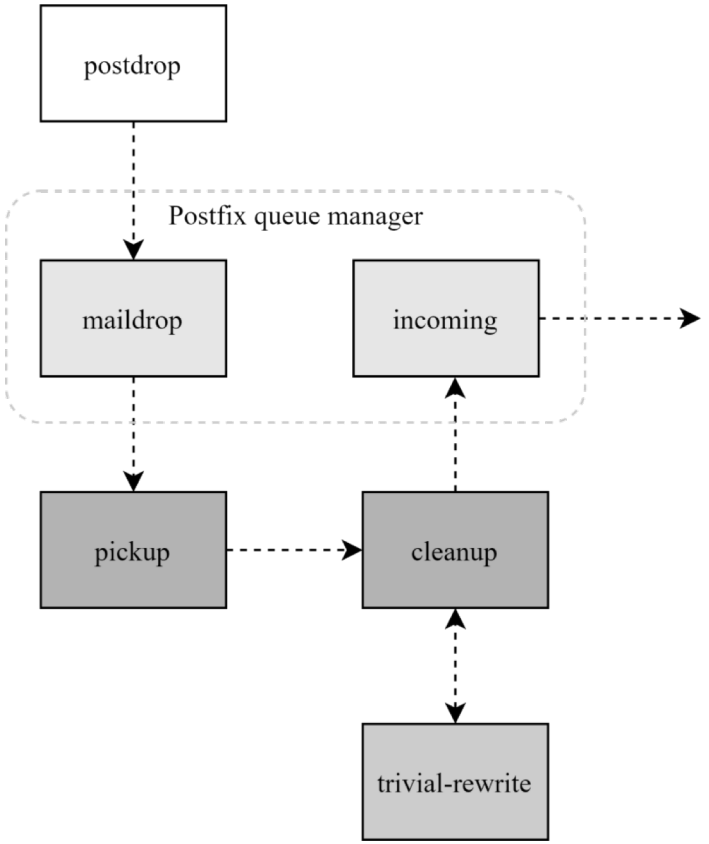
Postfix Architecture

- 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

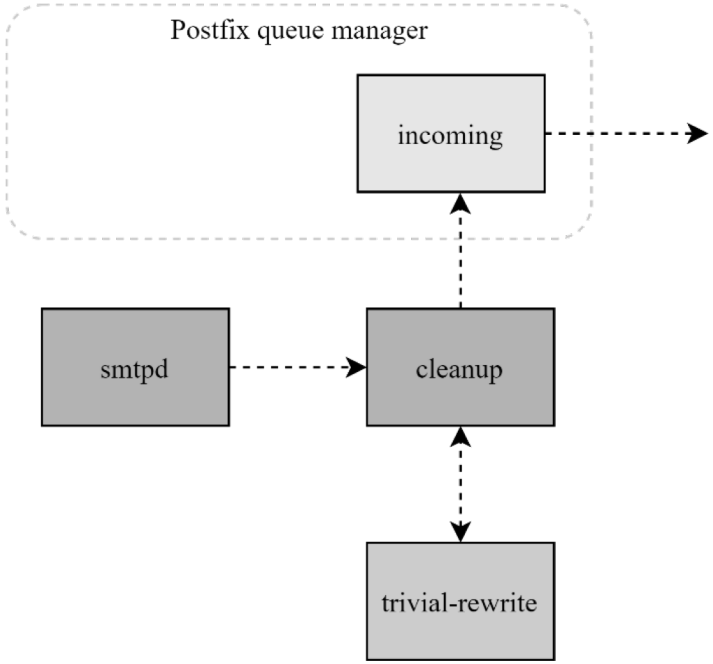


Postfix Architecture – Message IN

- Four ways
  - Local submission
    - postdrop command
    - maildrop queue
    - pickup daemon
    - cleanup daemon
      - Header validation
      - Address translation
    - incoming queue
  - Network submission
    - smtpd daemon
  - Local forwarding
    - Resubmit for such as .forward
    - Envelope "to" is changed
  - Notification
    - Notify admin when error happens



Local submission



Network submission

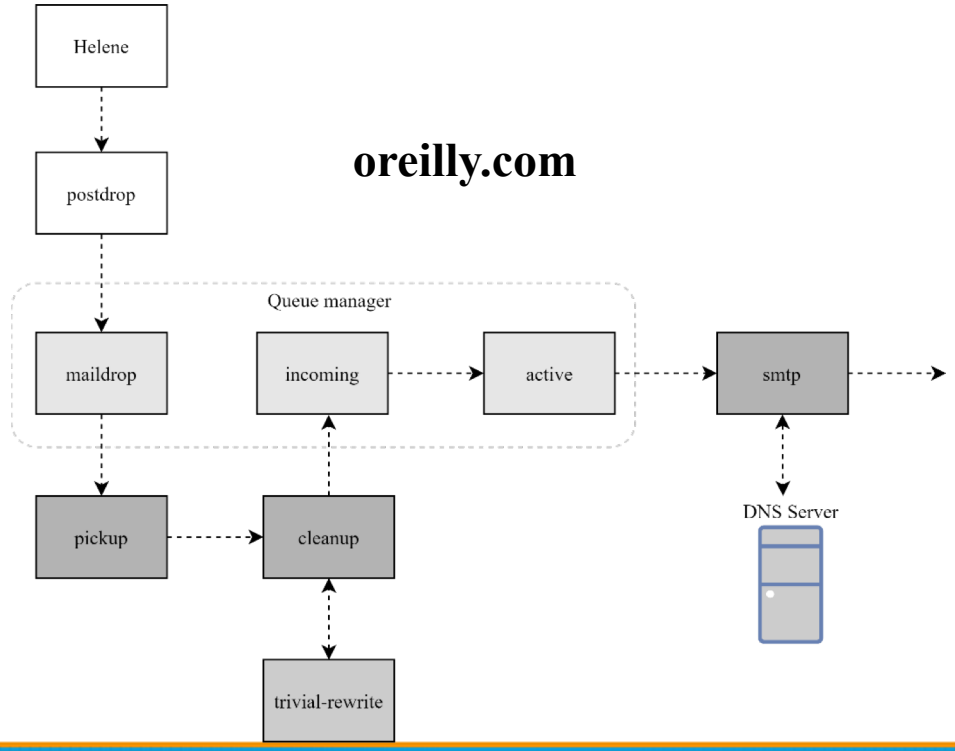
Postfix Architecture – Queue

- 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
    - Requested by admin (manually or automatically)
    - Stay in queue until admin intervenes

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

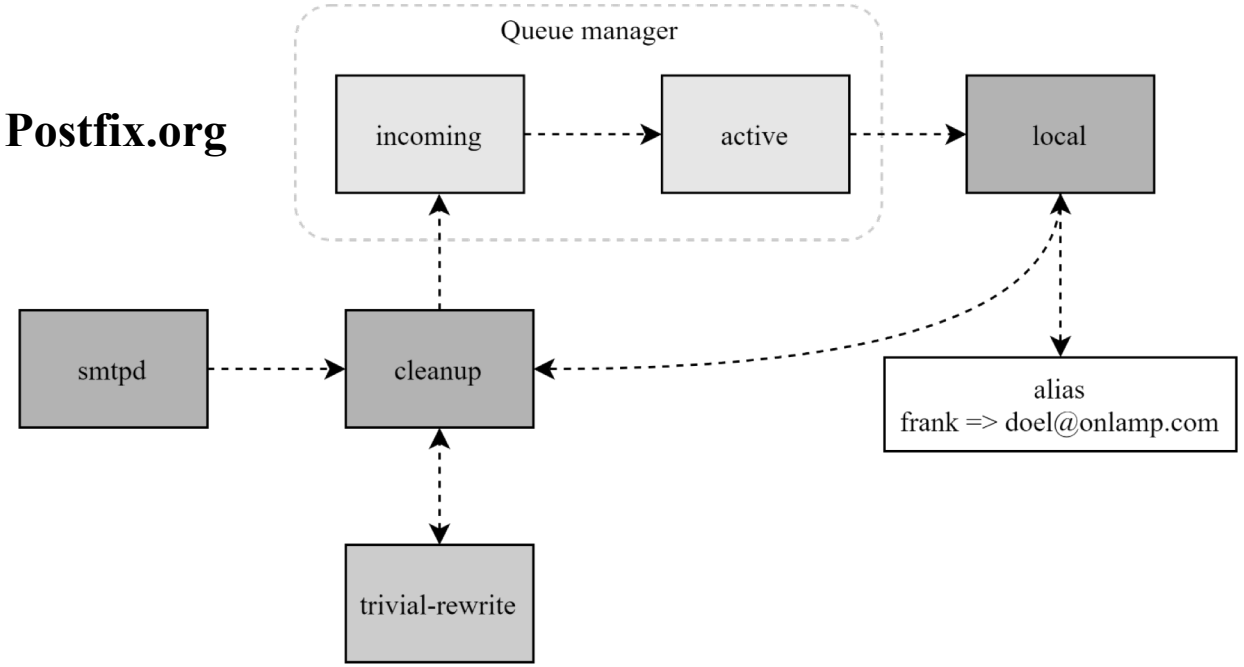
Message Flow in Postfix (1)

- 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



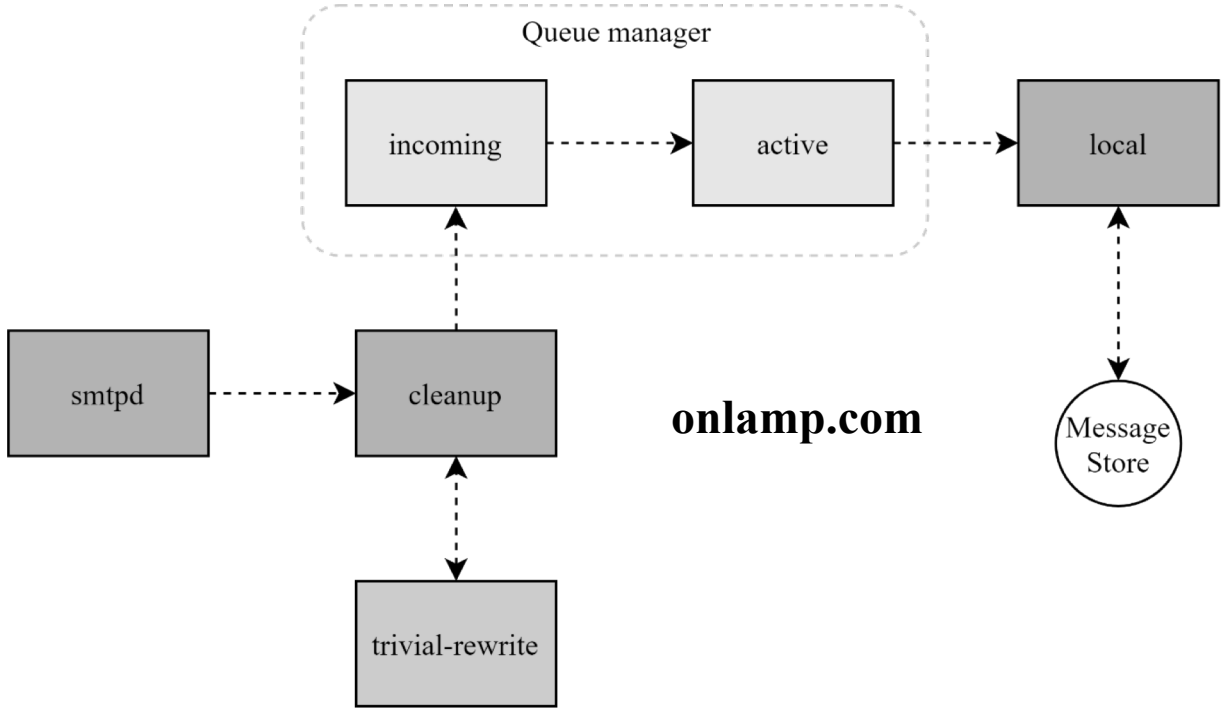
Message Flow in Postfix (2)

- Example
  - frank@postfix.org => doel@onlamp.com
  - 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)

- Example
  - frank@postfix.org => doel@onlamp.com
  - Phase3
    - The smtpd on onlamp.com takes this message and invoke cleanup then put in incoming queue
    - Local delivery to message store



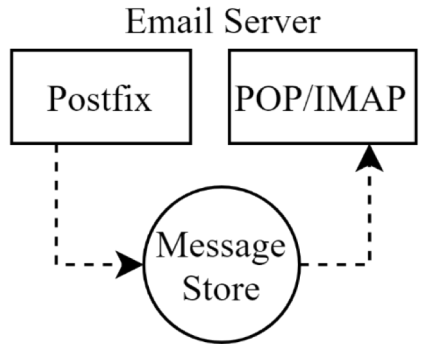
Message Store Format

- 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 (performance)
- The Maildir format
  - Use structure of directories to store email messages
  - Each message is in its owned file
  - Three subdirectories - cur, new, and tmp
    - cur: already read
    - new: unread
    - tmp: under receving (working dir)
  - Maildir format has scalability problem
    - locate and delete mails quickly, but waste amounts of fd, inodes, space
    - Problems of quota and backup
- Related parameters (in main.cf)
  - mail_spool_directory = /var/mail (Mbox)
  - mail_spool_directory = /var/mail/ (Maildir)

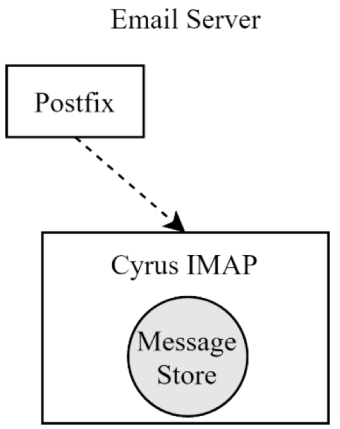
Read your mail from terminal

- To read mails, you must login via ssh
  - Built-in command to read mail: "mail"
  - Friendly command-line MUA: "mutt"
    - Pkg: mutt
    - Port: mail/mutt
- To read from remote host
  - Supports MUA like Outlook, Thunderbird, or even Gmail
  - You need MAA (supports IMAP/POP3)
  - Dovecot
    - Pkg: dovecot
    - Port: mail/dovecot

Postfix & POP3/IMAP



- POP3 vs. IMAP
  - Both are used to retrieve mail from server for remote clients
  - POP3 has to download entire message, while IMAP can download headers only
  - POP3 can download only single mailbox, while IMAP can let you maintain multiple mailboxes and folders on server
- Postfix works together with POP3/IMAP
  - Postfix and POP3/IMAP must agree on the type of mailbox format and style of locking
    - Standard message store
    - Non-standard message store
      - Such as Cyrus IMAP or Dovecot



Postfix Configuration

- Two most important configuration files
  - /usr/local/etc/postfix/main.cf – postconf(5)
    - Core configuration
  - /usr/local/etc/postfix/master.cf – master(5)
    - Which postfix service should invoke which program
- Edit main.cf
  - Using text editor
  - postconf
    - $ postconf [-e] "myhostname=nasa.cs.nctu.edu.tw"
    - $ postconf -d myhostname (print default setting)
    - $ postconf myhostname (print current setting)
- Reload postfix whenever there is a change
  - $ postfix reload

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
- Database format
  - $ postconf -m
    - List all available database format
  - In main.cf
    - default_database_type

```
$ postconf  default_database_type
default_database_type = hash
$ postconf  -h default_database_type
hash
```

```
% postconf -m
btree
cidr
environ
hash
internal
proxy
regexp
static
tcp
texthash
unix
```

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

Postfix Configuration – Lookup tables (2)

- Use databased-lookup table in main.cf
  - syntax

    parameter = type:name
  - E.g.
    - In main.cf
      canonical_maps = hash:/usr/local/etc/postfix/canonical
    - After execute postmap
      /usr/local/etc/postfix/canonical.db
- postmap command
  - Generate database
    - $ postmap hash:/usr/local/etc/postfix/canonical
  - Query
    - $ postmap -q nctu.edu.tw hash:/usr/local/etc/postfix/canonical

don’t need to add ".db" here

Postfix Configuration – Lookup tables (3)

- Regular expression tables
  - More flexible for matching keys in lookup tables
    - Sometimes you cannot list all the possibilities
  - Two regular expression libraries used in Postfix
    - POSIX extended regular expression (regexp, default)
    - Perl-Compatible regular expression (PCRE)
  - Usage
    - /pattern/ value
    - Do some content checks (filtering)
      - header_checks
      - body_checks
    - Design some features
      - /(\S+)\.(\S+)@cs\.nctu\.edu\.tw/ $1@cs.nctu.edu.tw

Postfix Configuration – Categories

- Categories
  - Server identities
    - my...
  - Mail rewriting
    - for incoming/outgoing mails
  - Access control
    - restrictions
  - Mail processing
    - filter
  - Operation details
    - …

Postfix Configuration – MTA Identity

- Four related parameters
  - myhostname
    - myhostname = nasa.cs.nctu.edu.tw
    - If un-specified, postfix will use ‘hostname’ command
  - 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 = $myhostname www.$mydomain, ftp.$mydomain
  - mydomain
    - mydomain = cs.nctu.edu.tw
    - If un-specified, postfix use myhostname minus the first component
  - myorigin
    - myorigin = $mydomain (default is $myhostname)

Postfix Configuration – System-wide aliases

- Using aliases in Postfix (first-matching)
  - alias_maps = hash:/etc/aliases
  - alias_maps = hash:/etc/aliases, nis:mail.aliases
  - alias_database = hash:/etc/aliases
- alias_map vs alias_database
  - alias_map
    - Which map to use (lookup table)
    - Not all of them is controlled by Postfix
      - E.g. nis
  - alias_database
    - Tell "newaliases" which (local) database to rebuild

Postfix Configuration – System-wide aliases

- To Build alias database file
  - $ postalias /etc/aliases
    - Can be used on files other than /etc/aliases
  - $ newaliases
    - For /etc/aliases => can be changed by "alias_database"
- Alias file format (same as sendmail)
  - Value can be
    - Email address, filename, |command, :include:
- Alias restriction (alias, forward, include)
  - allow_mail_to_commands = alias, forward
  - allow_mail_to_files = alias, forward

Postfix Configuration – Virtual Alias Maps

- Virtual Alias Map
  - It recursively rewrites envelope recipient addresses for all local, all virtual, and all remote mail destinations.
  - virtual_alias_domains = $virtual_alias_maps (default)
  - virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
    - src-address dst-address

    lctseng@cs.nctu.edu.tw @nasa.cs.nctu.edu.tw

    lctseng alice@gmail.com

    @cs.nycu.edu.tw @cs.nctu.edu.tw
  - Applying regular expression
    - virtual_alias_maps = pcre:/usr/local/etc/postfix/virtual

    /^root(\..+)?@(t)?(cs|np)?bsd\d*\.cs\.nctu\.edu\.tw$/ bsdta@cs.nctu.edu.tw

    /^root(\..+)?@(t)?(cs|np)?linux\d*\.cs\.nctu\.edu\.tw$/ linuxta@cs.nctu.edu.tw

    /^root(\..+)?@(t)?csmail\w*\d*\.cs\.nctu\.edu\.tw$/ mailta@cs.nctu.edu.tw

Postfix Configuration – Virtual Alias Maps vs Alias Map

- alias_map
  - Used by local(8) delivery
  - Key must be local recipients
  - Value can be email/file/command/…
- virtual_alias_maps
  - Used by virtual(5) delivery
  - Higher priority than alias_map
  - Key can be
    - user@domain
    - user
    - @domain
  - Value must be valid email addresses or local recipients

Postfix Configuration – Relay Control (1)

- Open relay
  - A mail server that permit anyone to relay mails
    - Neither originates or ends with a user from its domain
    - Spam
  - By default, postfix is not an open relay

- A mail server should
  - Relay mail for trusted user
    - Such as lctseng@smtp.cs.nctu.edu.tw
  - Relay mail for trusted domain
    - E.g. *smtp.cs.nctu.edu.tw* trusts *cs.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, configured in this machine
  - mynetworks_style = host
    - Allow relaying for only local machine
  - mynetworks_style = class
    - Any host in the same class A, B or C
    - Usually we don't use this - your server may trust the whole subnet from your provider

Postfix Configuration – Relay Control (3)

- Restricting relay access by mynetworks (override mynetworks_style)
  - List individual IP or subnets in network/netmask notation
  - E.g. in /usr/local/etc/postfix/mynetworks
    - 127.0.0.0/8
    - 140.113.0.0/16
    - 10.113.0.0/16
- Relay depends on the type of your mail server
  - smtp.cs.nctu.edu.tw will be different from csmx1.cs.nctu.edu.tw
    - Outgoing: usually accepts submission from local domain
    - Incoming: may relay mails for trusted domains

Postfix Configuration – Rewriting address (1)

- For unqualified address
  - To append "myorigin" to local name
    - lctseng => lctseng**@nasa.cs.nctu.edu.tw**
    - append_at_myorigin = yes
  - To append "mydomain" to address that contain only host.
    - lctseng@nasa=> lctseng@nasa**.cs.nctu.edu.tw**
    - append_dot_mydomain = yes

Postfix Configuration – Rewriting address (2)

- Masquerading hostname
  - Hide the names of internal hosts to make all addresses appear as if they come from the same mail server
  - It is often used in out-going mail gateway
    - masquerade_domains = cs.nctu.edu.tw
      - lctseng@subdomain.cs.nctu.edu.tw => lctseng@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 (the default)
    - masquerade_class = envelope_sender, header_sender, header_recipient
    - This allows incoming messages can be filtered based on their recipient address

Postfix Configuration – Rewriting address (3)

- Canonical address – canonical(5)
  - Rewrite both header and envelope recursively invoked by cleanup daemon
  - In main.cf
    - canonical_maps = hash:/usr/local/etc/postfix/canonical
    - canonical_classes = envelope_sender, envelope_recipient, header_sender, header_recipient
  - In canonical

    /^(.*)@(t)?(cs)?(bsd|linux|sun)\d*\.cs\.nctu\.edu\.tw$/ $1@cs.nctu.edu.tw

  - Simlar configurations
    - sender_canonical_maps、sender_canonical_classes
    - recipient_canonical_maps、recipient_canonical_classes

Postfix Configuration – Rewriting address (4)

- Relocated users
  - Used to inform sender that the recipient is moved
    - "user has moved to *new_location*" bounce messages
  - In main.cf
    - relocated_maps = hash:/usr/local/etc/postfix/relocated
  - In relocated

    andy@nasa.cs.nctu.edu.tw andyliu@abc.com
    lctseng EC319, NCTU, Hsinchu, ROC
    @nabsd.cs.nctu.edu.tw zfs.cs.nctu.edu.tw

    Value can be anything: phone number, street address, …
- Unknown users
  - Not local user and not found in maps
  - Default action: reject

Postfix Configuration – master.cf (1)

- /usr/local/etc/postfix/master.cf (master(5))
  - Define services that **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    unix  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
rewrite   unix  -       -       n       -       -       trivial-rewrite
smtp      unix  -       -       n       -       -       smtp
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
relay     unix  -       -       n       -       -       smtp
        -o smtp_fallback_relay=
lmtp      unix  -       -       n       -       -       lmtp
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
```

Postfix Configuration – master.cf (2)

- Configuration options
  - Service name
  - Service type
    - inet, unix, fifo (obsolete), or pass
  - Private
    - Access to this component is restricted to the Postfix system
      - "inet" type cannot be private
  - Unprivileged
    - Run with the least amount of privilege required
      - y will run with the account defined in "mail_owner"
      - n will run with root privilege
        - local, pipe, spawn, and virtual

Postfix Configuration – master.cf (3)

- Configuration options
  - Chroot
    - chroot location is defined in "queue_directory"
  - Wake up time
    - Automatically wake up the service after the number of seconds
  - Process limit
    - Number of processes that can be executed simultaneously
    - Default count is defined in "default_process_limit"
  - command + args
    - Default path is defined in "daemon_directory"
      - /usr/libexec/postfix

Postfix Architecture – Message OUT

- Local delivery
- Relay to the destinations
- 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
  - lmtp
    - Local Mail Transfer Protocol (Limited SMTP)
      - No queue
      - One recipient at once
    - Used to deliver to mail systems on the same network or even the same host
  - pipe
    - Used to deliver message to external program

Mail Relaying – Transport Maps (1)

- Transport maps – transport(5)
  - It override default transport method to deliver messages
  - In main.cf
    - transport_maps = hash:/usr/local/etc/postfix/transport
  - In transport file
    - domain_or_addresstransport:nexthop

"Service" defined in master.cf

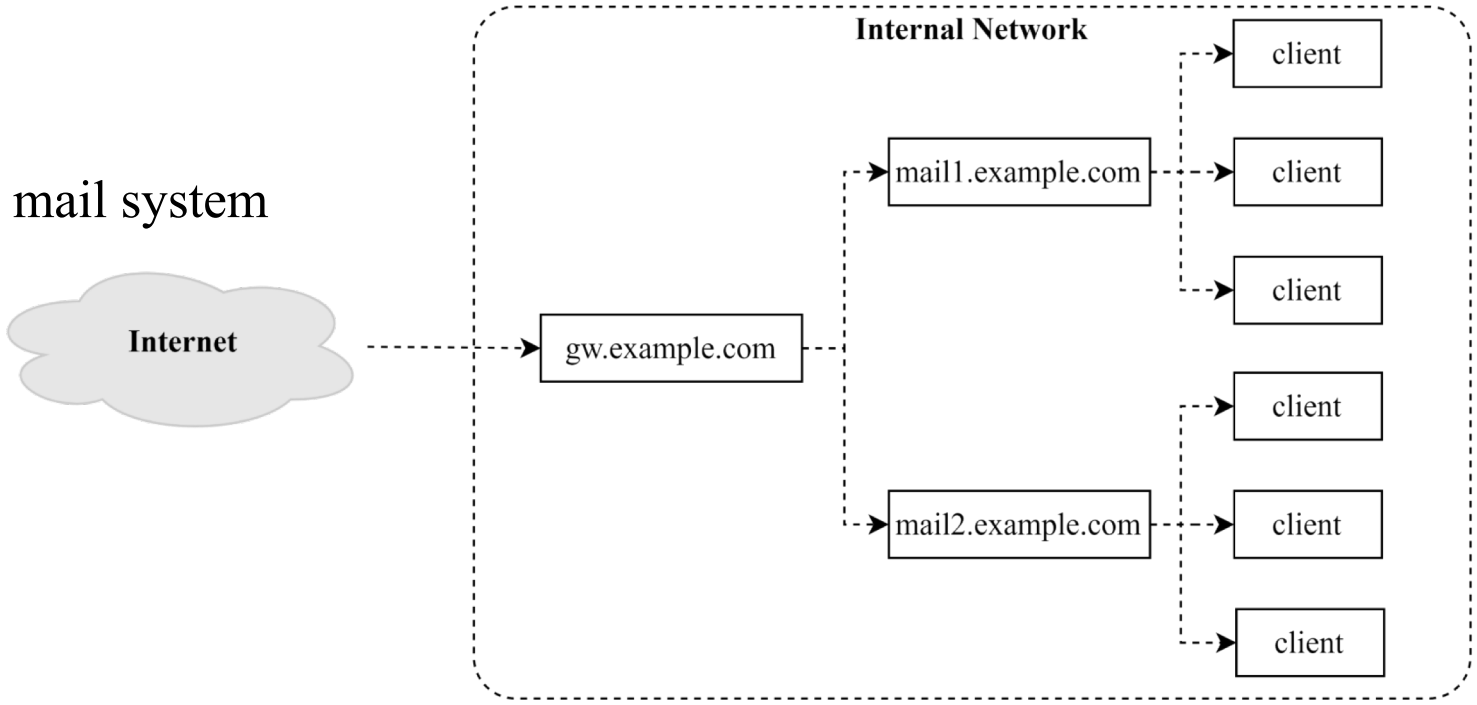
csie.nctu.edu.tw	smtp:[mailgate.csie.nctu.edu.tw]
cs.nctu.edu.tw	smtp:[csmailgate.cs.nctu.edu.tw]
cis.nctu.edu.tw	smtp:[mail.cis.nctu.edu.tw]
example.com	smtp:[192.168.23.56]:20025
orillynet.com	smtp
ora.com	maildrop
kdent@ora.com	error:no mail accepted for kdent

Mail Relaying – Transport Maps (2)

- Usage in transport map
  - MX => Local delivery mail server
  - mailpost to bbs/news
  - Postponing mail relay
    - Such as ISP has to postpone until customer network is online
    - In transport map:
      abc.com ondemand
    - In /usr/local/etc/postfix/master.cf
      ondemand unix - - n - - smtp
    - In /usr/local/etc/postfix/main.cf
      defer_transports = ondemand ← "ondemand" transport should trigger by postqueue
      transport_maps = hash:/usr/local/etc/postfix/transport
    - Whenever the customer network is online, do
      - $ postqueue -s abc.com

Mail Relaying – Inbound Mail Gateway (1)

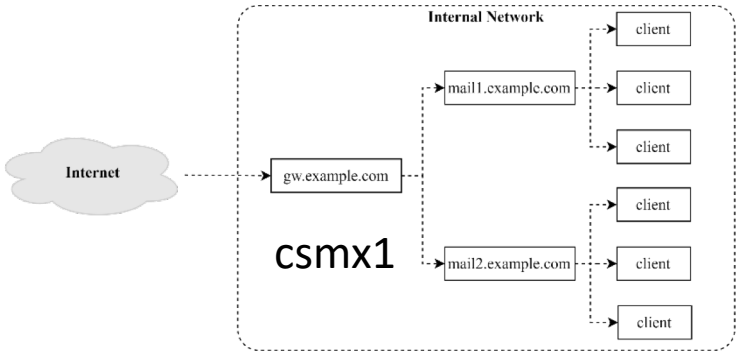
- Inbound Mail Gateway (IMG, MX)
  - Accept all mail for a network from the Internet and relays it to internal mail systems
  - E.g.
    - gw.example.com is a IMG
      - With MX records
    - mail1.example.com is internal mail system
      - Serves internal subnet



Mail Relaying – Inbound Mail Gateway (2)

- To be IMG, suppose
  - You are administrator for cs.nctu.edu.tw
  - Hostname is csmx1.cs.nctu.edu.tw
  - You have to be the IMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw
    - Firewall only allow outsource connect to IMG port 25

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



javaLab
secureLab

Mail Relaying – Outbound Mail Gateway

- Outbound Mail Gateway
  - Accept mails from inside network and relay them to Internet hosts
- To be OMG, suppose
  - You are administrator for cs.nctu.edu.tw
  - Hostname is csmailer.cs.nctu.edu.tw
  - You have to be the OMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw

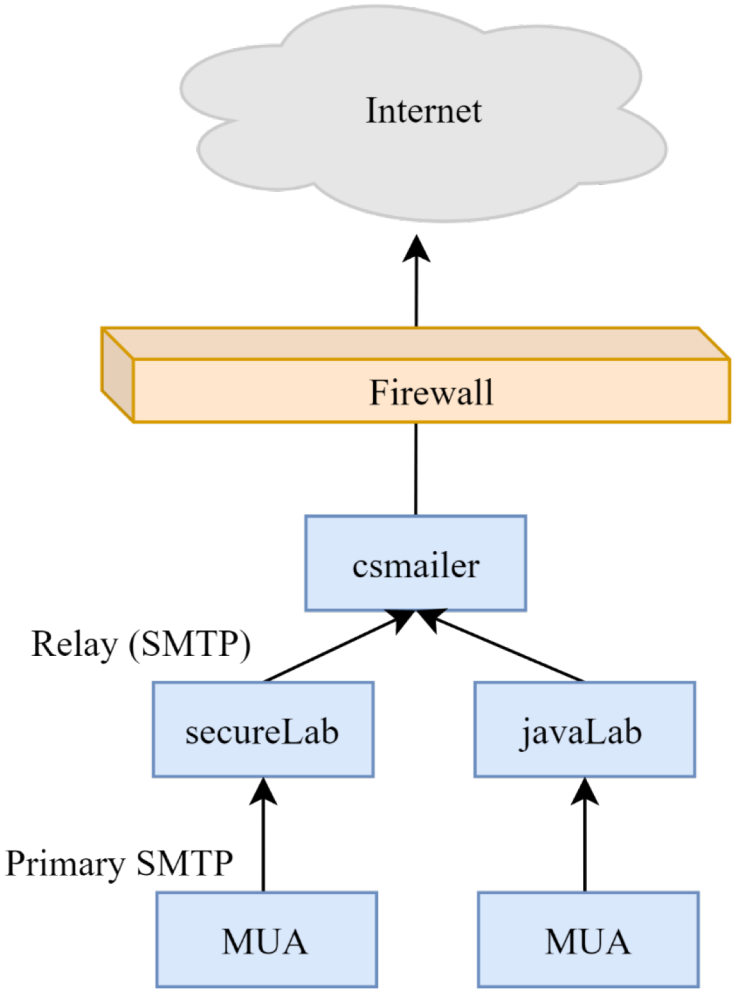
1. In main.cf of csmailer.cs.nctu.edu.tw

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

   ```
   secureLab.cs.nctu.edu.tw
   javaLab.cs.nctu.edu.tw
   ```

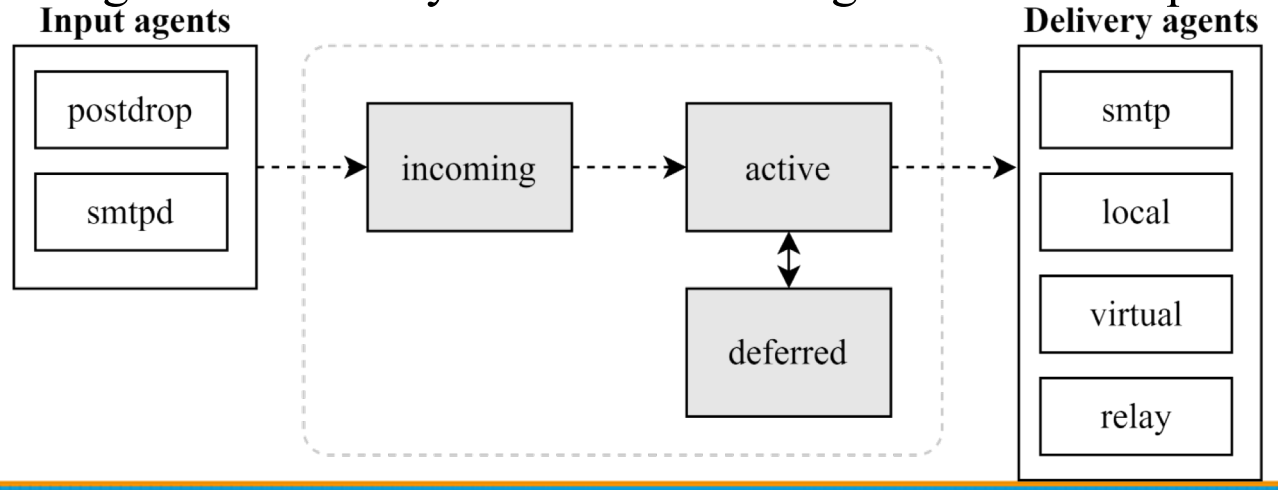
2. All students in secureLab/javaLab will configure their MUA to use secureLab/javaLab.cs.nctu.edu.tw to be the SMTP server
3. In main.cf of secureLab/javaLab.cs.nctu.edu.tw,

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



Queue Management

- The queue manage daemon
  - qmgr daemon
  - Unique queue ID
  - Queue directories (/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 = 300s
    - maximal_backoff_time = 4000s
  - qmgr daemon periodically scan deferred queue for reborn messages
    - queue_run_delay = 300s
- Deferred => bounce
  - maximal_queue_lifetime = 5d

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
    - You can override the default_destination_concurrency_limit for any transport mailer:
      - smtp_destination_concurrency_limit = 25 for external delivery
      - local_destination_concurrency_limit = 10 for local recipients
  - 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

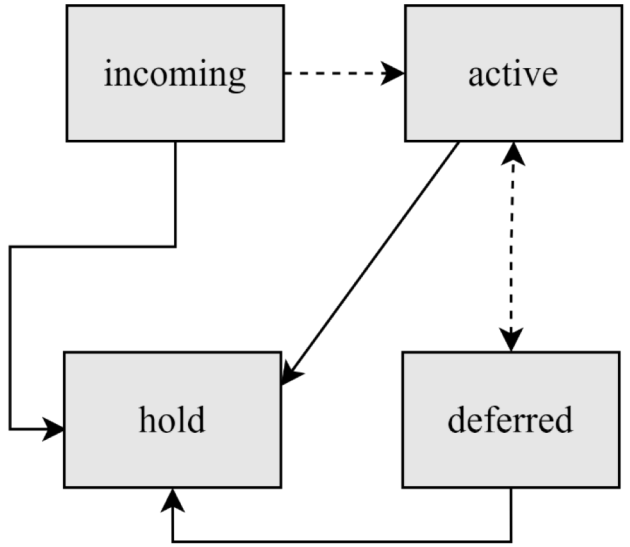
Queue Management – Error Notification

- 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	2bounce_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 problem	error_notice_recipient
software	Send notice because of software problem	error_notice_recipient

Queue Management – Queue Tools (1)

- postqueue(1)
  - postqueue –p (or mailq)
    - Show the queued mails (with information like message ID, but not mail content)
  - postqueue –f
    - Attempt to flush(deliver) all queued mail
  - postqueue –s cs.nctu.edu.tw
    - Schedule immediate delivery of all mail queued for site
- postsuper(1)
  - Delete queued messages
    - postsuper –d E757A3428C6 (from incoming, active, deferred, hold)
    - postsuper –d ALL
  - Put messages "on hold" so that no attempt is made to deliver it
    - postsuper –h E757A3428C6 (from incoming, active, deferred)
  - Release messages in hold queue (into deferred queue)
    - postsuper –H ALL
  - Requeue messages into maildrop queue (maildrop => pickup => cleanup => incoming)
    - postsuper –r E757A3428C6
    - postsuper –r ALL



Queue Management – Queue Tools (2)

- postcat(1)
  - Display the contents of a queue file

```
nasa [/home/lctseng] -lctseng- mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
3314234284A      602 Sat May 19 04:16:20  root@nasa.cs.nctu.edu.tw
    (connect to csmx1.cs.nctu.edu.tw[140.113.235.104]:25: Operation timed out)
                                         lctseng@cs.nctu.edu.tw

nasa [/home/lctseng] -lctseng- sudo postcat -q 3314234284A
*** ENVELOPE RECORDS deferred/3/3314234284A ***
message_size:             602             214                1               0             602
message_arrival_time: Sat May 19 04:16:20 2012
create_time: Sat May 19 04:16:20 2012
sender: root@nasa.cs.nctu.edu.tw
named_attribute: rewrite_context=local
original_recipient: root
recipient: lctseng@cs.nctu.edu.tw
*** MESSAGE CONTENTS deferred/3/3314234284A ***
Received: by nasa.cs.nctu.edu.tw (Postfix)
        id 3314234284A; Sat, 19 May 2012 04:16:20 +0800 (CST)
Delivered-To: root@nasa.cs.nctu.edu.tw
Received: by nasa.cs.nctu.edu.tw (Postfix, from userid 0)
        id 2CB713427A5; Sat, 19 May 2012 04:16:20 +0800 (CST)
To: root@nasa.cs.nctu.edu.tw
Subject: nasa.cs.nctu.edu.tw weekly run output
Message-Id: <20120518201620.2CB713427A5@nasa.cs.nctu.edu.tw>
Date: Sat, 19 May 2012 04:16:20 +0800 (CST)
From: root@nasa.cs.nctu.edu.tw (NASA Root)

Rebuilding locate database:

Rebuilding whatis database:
    …
```

Multiple Domains

- Use single system to host many domains
  - E.g.
    - We use csmailgate.cs.nctu.edu.tw to host both **cs.nctu.edu.tw** and **csie.nctu.edu.tw**
  - Purpose
    - Final delivery on the machine
    - Forwarding to destination elsewhere (mail gateway)
- 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 (lctseng@ => /var/mail/lctseng)
- Procedure
  - Setup MX records for both domains
  - Modify "mydomain" to canonical domain
  - Modify "mydestination" parameter to let mails to virtual domain can be local delivered
  - E.g.
    - 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
  - 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
  - E.g.
    - mydomain = cs.nctu.edu.tw
    - virtual_alias_domains = abc.com.tw, xyz.com.tw
    - virtual_alias_maps = hash:/usr/local/etc/postfix/virtual

- Limitation
  - Need to maintain system accounts for virtual domain users

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
  - Modify "virtual_mailbox_base" and create related directory to put mails
  - Create "virtual_mailbox_maps" map
  - E.g.
    - virtual_mailbox_domain = abc.com.tw, xyz.com.tw
    - virtual_mailbox_base = /var/vmail
    - Create /var/vmail/abc-domain and /var/vmail/xyz-domain
    - virtual_mailbox_maps = hash:/usr/local/etc/postfix/vmailbox

    - In /usr/local/etc/postfix/vmailbox
      - CEO@abc.com.tw abc-domain/CEO (Mailbox format)
      - CEO@xyz.com.tw xyz-domain/CEO/ (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
    - E.g.
      - virtual_uid_maps = static:1003
      - virtual_gid_maps = static:105

      - virtual_uid_maps = hash:/usr/local/etc/postfix/virtual_uids
      - virtual_uid_maps = hash:/usr/local/etc/postfix/virtual_uids static:1003

      - In /usr/local/etc/postfix/virtual_uids
        - CEO@abc.com.tw 1004
        - CEO@xyz.com.tw 1008

Step by Step Examples

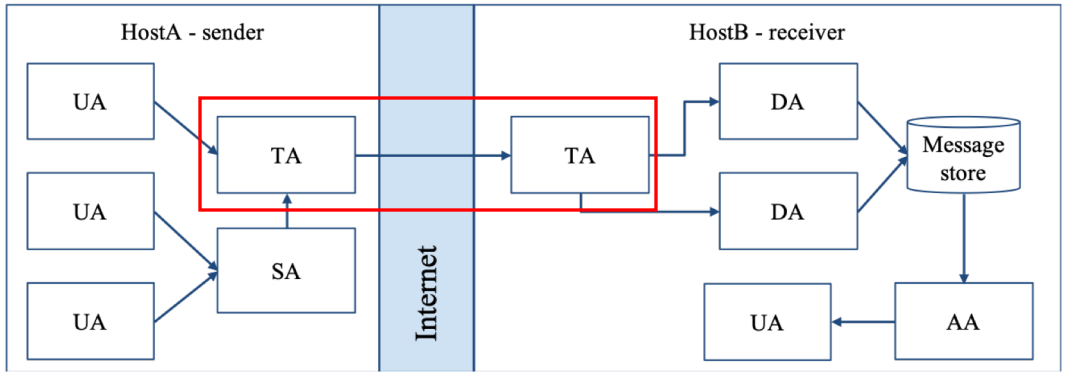
Let’s learn from examples

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

- Note
  - In this example, we assume you have public IP/domain

Build a Basic MTA



Can send mails to other domain

Build a basic MTA(1)

- Can send mails to other domain
- Install Postfix
  - Pkg: postfix
  - Port: mail/postfix
- 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(2)

- Replace sendmail by Postfix modified version
  - Edit /etc/mail/mailer.conf

```
Sendmail    /usr/local/sbin/sendmail
send-mail   /usr/local/sbin/sendmail
Mailq       /usr/local/sbin/sendmail
newaliases  /usr/local/sbin/sendmail
```

Build a basic MTA(3)

- 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(4)

- Set up 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)

Send test mails to verify your MTA(3)

- Mail source text of the previous 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
  - postqueue
  - postsuper

Check whether your mail is sent or not (2)

- Example for rejected mails (send mails to @cs.nctu.edu.tw)

```
-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 (default) in main.cf

```
mynetworks_style = host
```

  - So Postfix only trust clients from localhost

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 (need to enable it by port)
- References
  - http://wiki2.dovecot.org/
  - http://www.postfix.org/SASL_README.html

MTA authentication(3) - Dovecot SASL

- Installation
  - Pkg: dovecot
  - Port: mail/dovecot
- 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
    - Note: 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 {
  ...
  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
  }
  ...
}
```

  - 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 (backward) 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(2-3) - Set up SMTP over TLS

- Send mail with STARTTLS
  - You cannot use telnet (plain-text client) anymore
  - Connection becomes encrypted after STARTTLS
  - telnet cannot read encrypted text
- OpenSSL client

```
openssl s_client -connect demo1.nasa.lctseng.nctucs.net:25 -starttls smtp
```

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

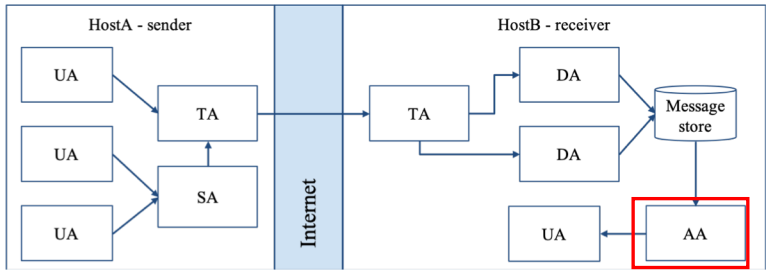
- Now you can use SSL clients to use SMTPs
  - telnet may not work in encrypted sessions
  - SSL client:

```
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 "mail from/rcpt to" instead of "MAIL FROM/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

國立陽明交通大學資工系資訊中心
Computer Center of Department of Computer Science, NYCU

MAA for POP3 and IMAP (1)

- 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: https://doc.dovecot.org/configuration_manual/quick_configuration/

MAA for POP3 and IMAP (2) - 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 (must agrees with Postfix)
  - 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 (3)

- 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

MAA for POP3 and IMAP (4)

- IMAP + STARTTLS

```
openssl s_client -connect host.example.com:143 -starttls imap
```

- POP3 + STARTTLS

```
openssl s_client -connect host.example.com:110 -starttls pop3
```

- IMAPs

```
openssl s_client -connect host.example.com:993
```

- POP3s

```
openssl s_client -connect host.example.com:995
```

- Sample message from Dovecot when succeed
  - POP `+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/