



# Postfix

tsaimh (2024-2025, CC-BY)  
lctseng (2020-2023, CC-BY)  
? (?-2019)

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

# Postfix

- Postfix is **Wietse Venema**'s mail server that started life at **IBM research** as an alternative to the widely-used **Sendmail** program.
- The software is also known by its former names **VMailer** and **IBM Secure Mailer**.
- The name **Postfix** is a compound of "**post**" (i.e., mail) and "**bugfix**" (for other software that inspired Postfix development).
- Postfix attempts to be **fast, easy to administer, and secure**.
- The **outside** has a definite **Sendmail-ish flavor**, but the **inside** is **completely different**.



Wietse Zweitze Venema

[Pronunciation](#)

# Postfix (cont.)

- After eight years at **Google**, Wietse continues to maintain Postfix.
- Postfix v3.9
  - First released in December 1998
  - Latest stable release: 3.10.1 (February 24, 2025 release)
  - `/usr/ports/mail/postfix`
  - `pkg install postfix`
- <http://www.postfix.org>
  - <http://www.postfix.org/documentation.html>

```
HISTORY
    The postqueue command was introduced with Postfix version 1.1.

AUTHOR(S)
    Wietse Venema
    IBM T.J. Watson Research
    P.O. Box 704
    Yorktown Heights, NY 10598, USA

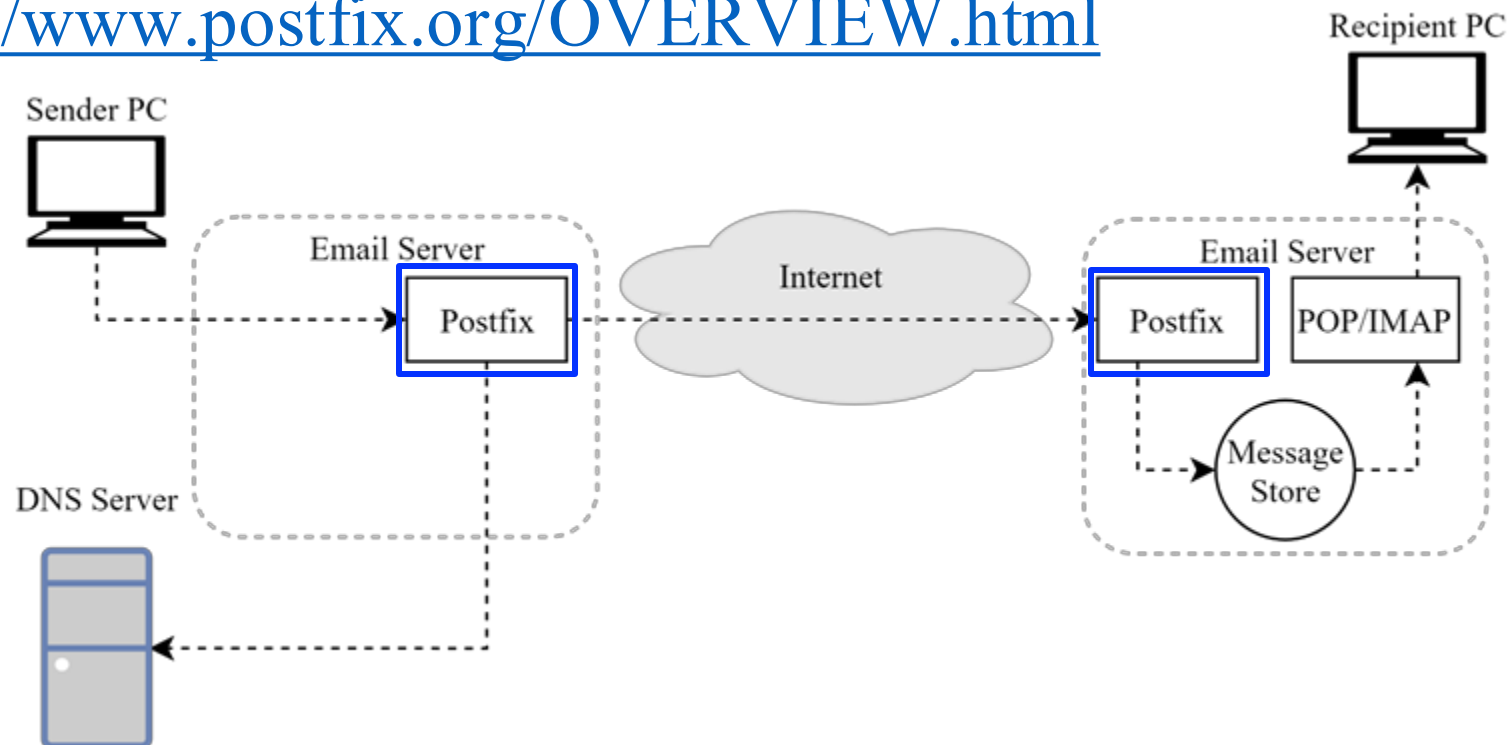
    Wietse Venema
    Google, Inc.
    111 8th Avenue
    New York, NY 10011, USA

(END)                                     POSTQUEUE(1)
```

Source: man page of postqueue(1)

# Role of Postfix

- MTA that
  - Receive and deliver email over the network (SMTP)
  - Local delivery
  - <http://www.postfix.org/OVERVIEW.html>

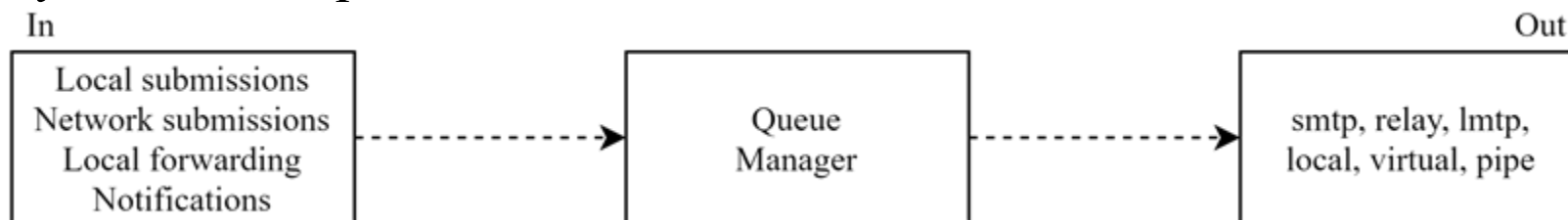




# Postfix Architecture (cont.)

- Modular-design MTA
  - Not a monolithic system (e.g. sendmail).
  - Several individual programs => each one handles specific task
  - Most important: “**master**”
    - Reside in memory (daemon)
    - Load configuration from [master.cf](#) and [main.cf](#)
    - Invoke other processes for tasks
- Major tasks
  - Receive mail and put in **queue** ([/var/spool/postfix](#))
  - Queue management
  - Delivery mail from queue

```
$ ls /var/spool/postfix
active      flush      private
bounce     hold       public
corrupt    incoming   saved
defer      maildrop   trace
deferred   pid
```

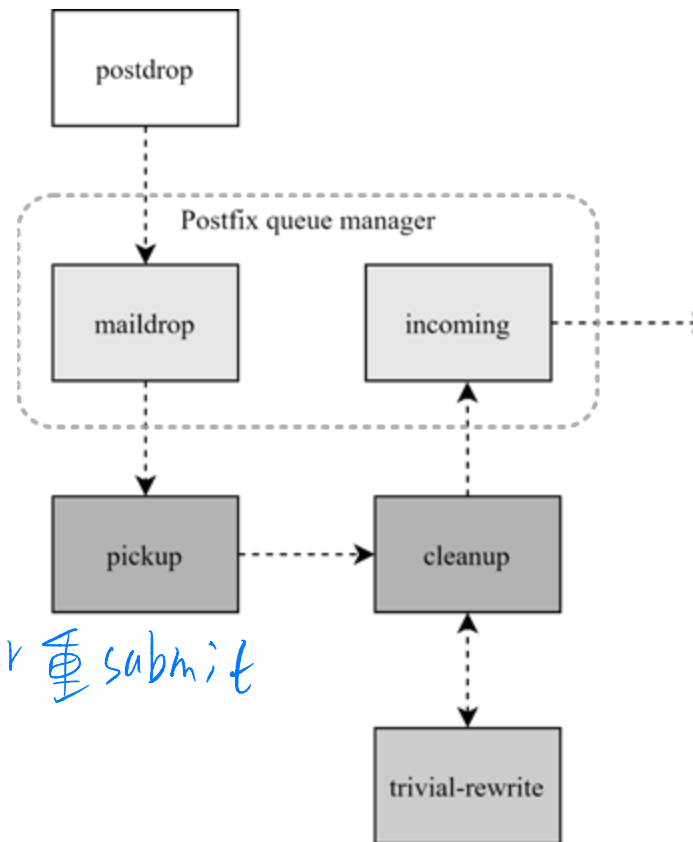


IMAP/POP3  
(沒有user account)

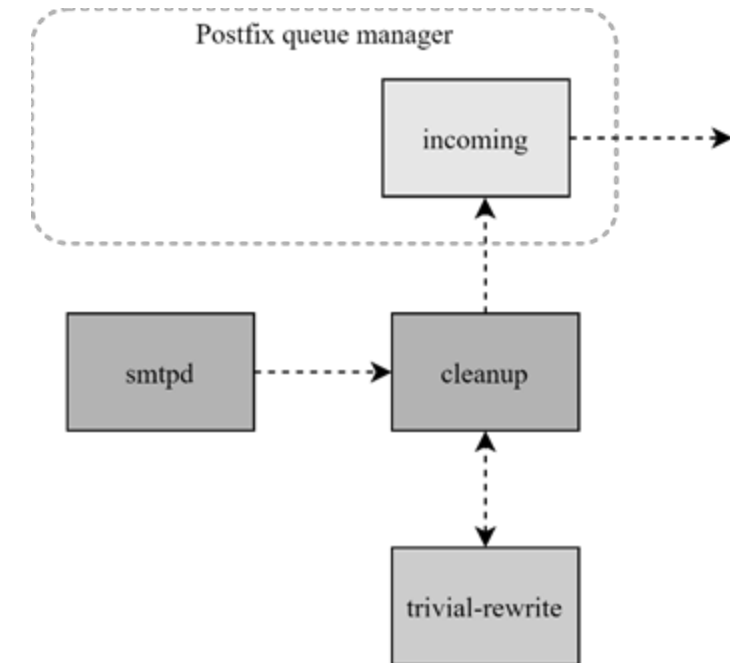
# Postfix Architecture – Message IN

- Four ways

- Local submission
  - “postdrop” command
  - “maildrop” queue
  - “pickup” daemon
  - “cleanup” daemon
    - Header/address validation
  - “incoming” queue
- Network submission
  - “smtpd” daemon
- Local forwarding
  - Resubmit for such as .forward *換 receiver 重 submit*
  - Envelope "to" is changed
- Notification
  - Notify admin when error happens



Local submission



Network submission

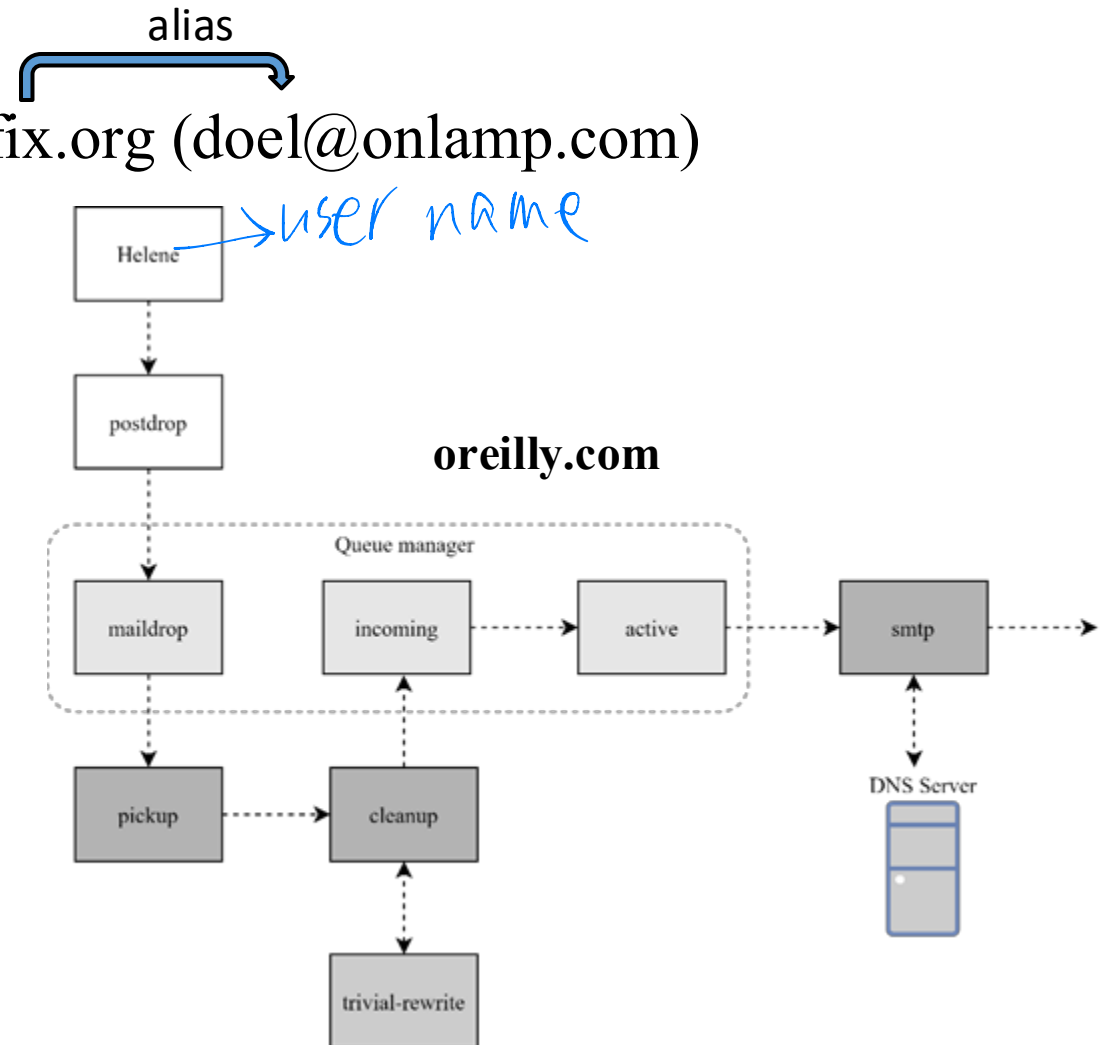
# Postfix Architecture – Queue

- 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** *↳ delivery agent*
    - ◻ 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

# Message Flow in Postfix (1)

- Example

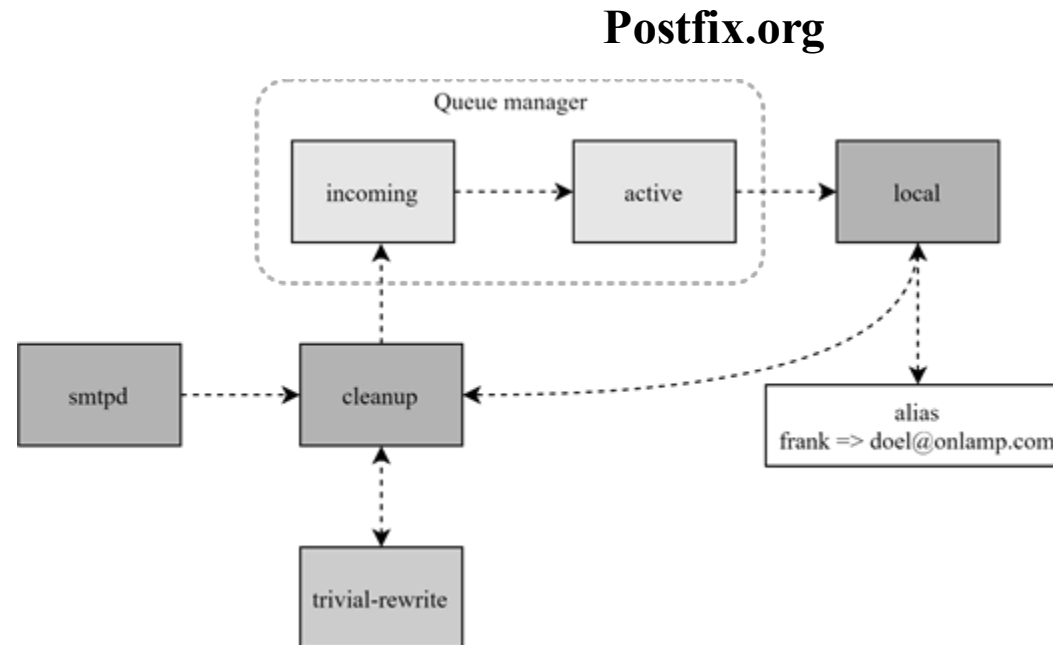
- `helene@oreilly.com => frank@postfix.org (doel@onlamp.com)`
- Phase 1:
  - Compose mail using MUA
  - Call `postdrop` command to send it
    - To “maildrop” queue



# Message Flow in Postfix (2)

- Example

- `frank@postfix.org => doel@onlamp.com`
- Phase2:
  - `smtpd` on `postfix.org`: receive message and invoke `cleanup`
  - “local” MDA find that `frank` is an alias => resubmits it through `cleanup` daemon

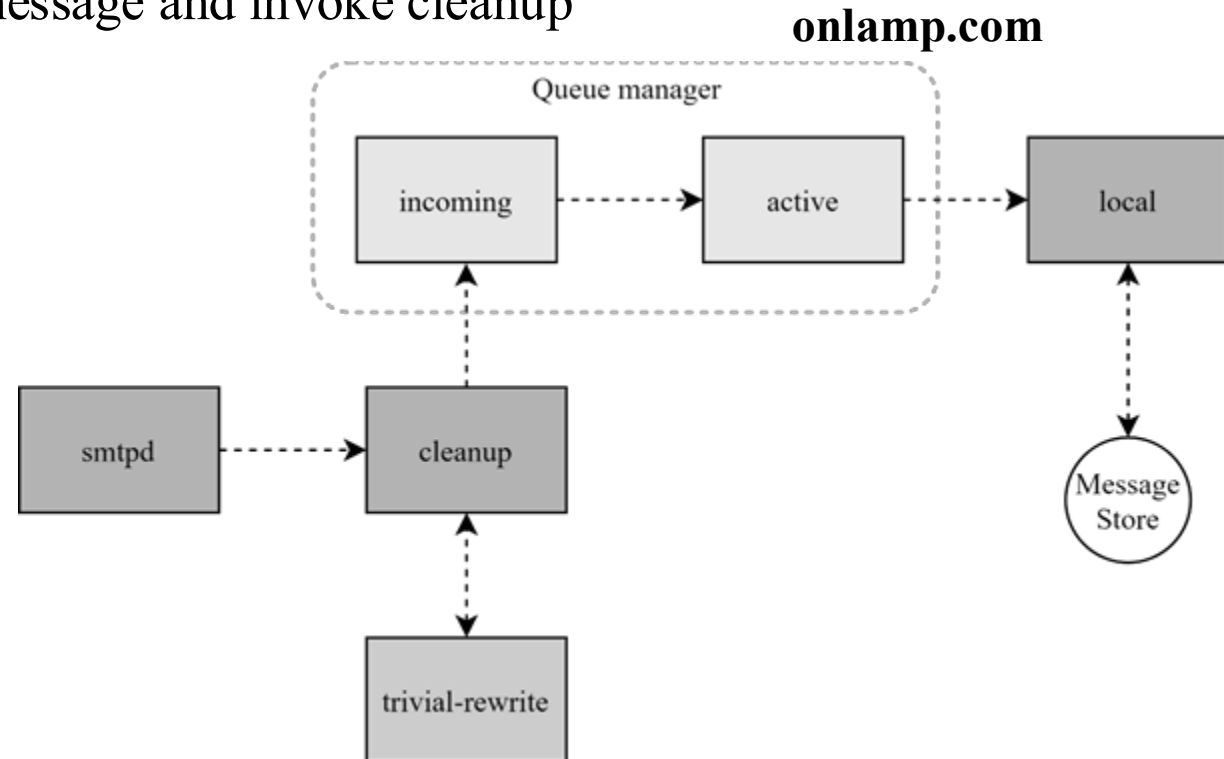


# Message Flow in Postfix (3)

- Example

- frank@postfix.org => doel@onlamp.com
- Phase3
  - smtpd on onlamp.com: receive message and invoke cleanup
  - Local delivery to message store

*/var/mail/[username]*



# Message Store Format

**mail\_spool\_directory** (default: see "postconf -d" output)  
The directory where [local\(8\)](#) UNIX-style mailboxes are kept. The default setting depends on the system type.  
Specify a name ending in / for maildir-style delivery.

- The **Mbox** format

- Store messages in **single file** for each user *=> in (each) line*
- 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 *=> in each file*
- Each message is in its own file
- Three subdirectories - cur, new, and tmp
  - cur: already read
  - new: unread
  - tmp: under receiving (working dir)
- Maildir format has **scalability** problem
  - locate and delete mails quickly, but waste amounts of fd, inodes, space
  - Problems of quota and backup*↳ 4k: inode + 4k data  
→ per 1 file*

# Message Store Format (cont.)

**mail\_spool\_directory** (default: see "postconf -d" output)

The directory where [local\(8\)](#) UNIX-style mailboxes are kept. The default setting depends on the system type.  
Specify a name ending in / for maildir-style delivery.

- Related parameters (in main.cf)

- `mail_spool_directory = /var/mail` (Mbox)
- `mail_spool_directory = /var/mail/` (Maildir)

```
tsaimh@bsd1:~ $ ls -l /var/mail/tsaimh
-rw----- 1 tsaimh tsaimh 51204482 Apr 15 09:25 /var/mail/tsaimh
tsaimh@bsd1:~ $ head -3 /var/mail/tsaimh
From tsaimh@imslab.org Tue Apr 23 14:51:46 2024
Return-Path: <tsaimh@imslab.org>
Received: from bsd1.imslab.org (localhost [127.0.0.1])
tsaimh@bsd1:~ $
```

# Mailbox Format Supported by Dovecot

⇒ extra mail/box format extension

Name	Tag	Description	
<u>obox</u>	obox	OX Dovecot Pro object storage mailbox format. (Pro only)	
<u>mbox</u>	mbox	Traditional UNIX mailbox format. Users' INBOX mailboxes are commonly stored in <code>/var/spool/mail</code> or <code>/var/mail</code> directory. Single file contains multiple messages.	
<u>Maildir</u>	maildir	One file contains one message. A reliable choice since files are never modified and all operations are atomic. The top-level Maildir directory contains the <code>Maildir/cur</code> , <code>Maildir/new</code> , and <code>Maildir/tmp</code> subdirectories.	
<u>dbx</u>	sdbox	<b>single-dbox</b> , one message per file.	Dovecot's own high performance mailbox format. Messages are stored in one or more files, each containing one or more messages.
	mdbox	<b>multi-dbox</b> , multiple messages per file.	
<u>imapc</u>	imapc	Use remote IMAP server as mail storage.	
<u>pop3c</u>	pop3c	Use remote POP3 server as mail storage.	

Supported by Postfix

# 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

send mail:

\$ mail -s "subject" mail/address  
content ...

^Z

# Postfix & POP3/IMAP



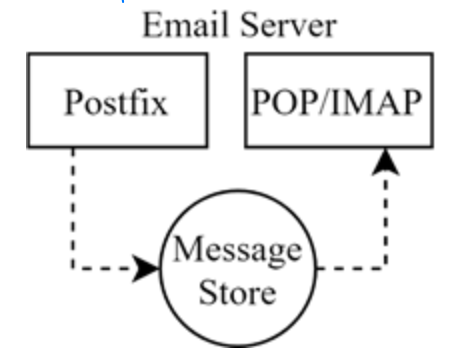
## • POP3 vs. IMAP

↳ Post office Protocol      ↳ Internet message access protocol

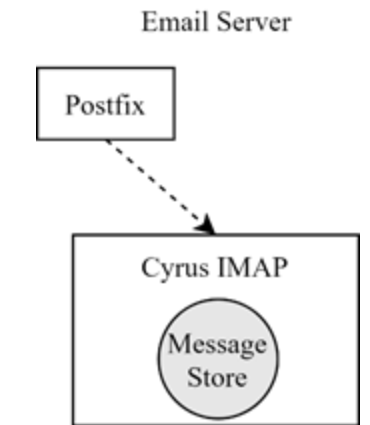
- Both are used to retrieve mail from server for remote clients
- **POP3** has to download **entire message**, while **IMAP** can **download headers** only
- **POP3** can download only **single mailbox**, while **IMAP** can let you maintain **multiple mailboxes and folders** on server

## • 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**



Standard message store



Non-standard message store

# 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.nycu.edu.tw"`
    - `$ postconf -d myhostname` (print default setting)
    - `$ postconf myhostname` (print current setting)
- Reload postfix whenever there is a change
  - `$ postfix reload`

```
$ hostname  
bsd1.imslab.org  
$ postconf -d myhostname  
myhostname = bsd1.imslab.org  
$ postconf myhostname  
myhostname = mx1.imslab.org
```

↳ `main.cf` (current setting)

# 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

*⇒ text-based ⇒ O(n)*

- Lookup tables** syntax

- Key values

*alias ⇒ key: value1, value2, ...*

- 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
```

*O(1)*

```
% postconf -m
btree
cidr ⇒ ip addr
environ
hash ⇒ common use
internal
proxy
regexp ⇒ common use
static
tcp
texthash
unix
```

# 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

→ db type that should be generate

- postmap command

- Generate database

- \$ postmap hash:/usr/local/etc/postfix/canonical

→ lookup table (text)

- 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

tsaimh.ABC@cs.nctu.edu.tw -> tsaimh@cs.nctu.edu.tw



Like the "+" sign used in Gmail

# 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 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)

postfix's default is not open relay

- Open relay

- A mail server that permit anyone to relay mails
  - Either 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 = host`
    - Allow relaying for only local machine (the default setting)
  - `mynetworks_style = subnet`
    - Allow relaying from other hosts in the same `subnet`, configured in this 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 ISP

# 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
```

- Similar 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=  
lmtpl unix - - n - - lmtpl  
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:nextthop`

 "Service" defined in master.cf

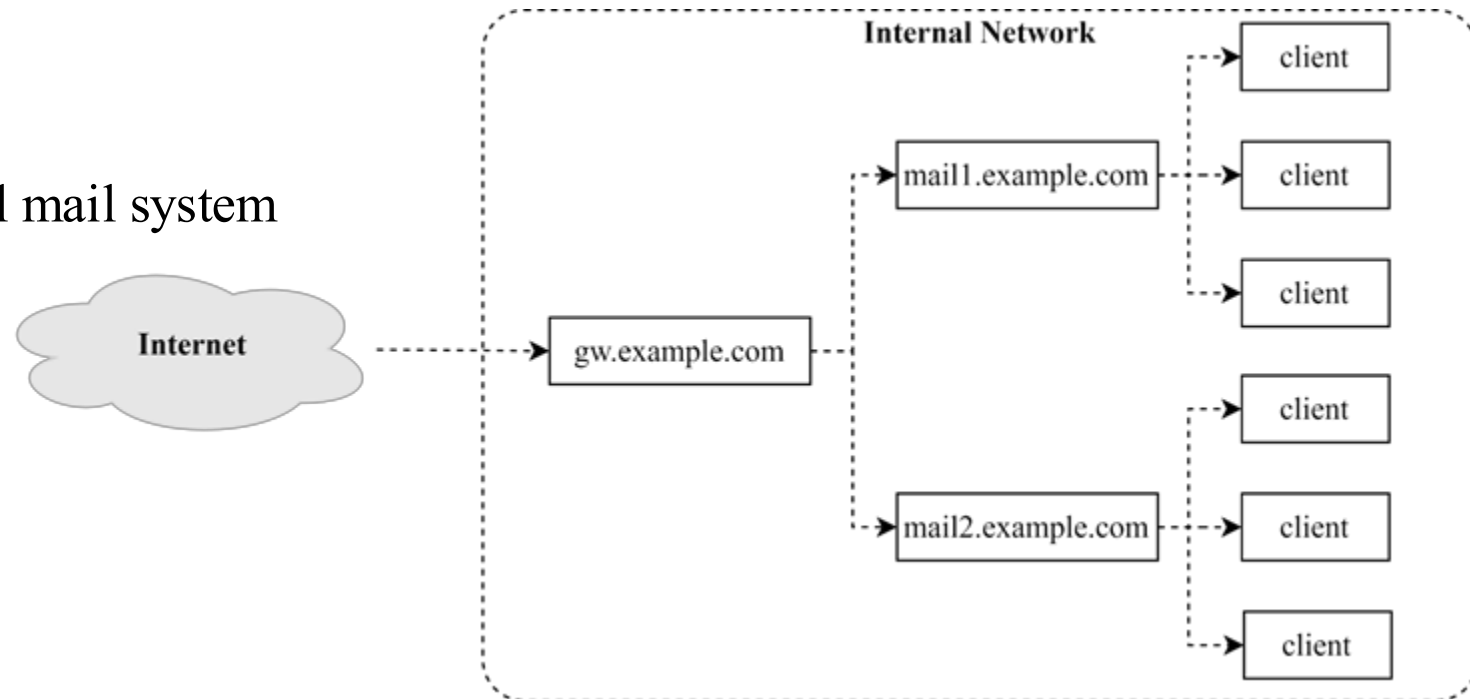
csie.nctu.edu.tw	smtp:[mailgate.csie.nctu.edu.tw]
cs.nctu.edu.tw	smtp:[csmailgate.cs.nctu.edu.tw]
cis.nctu.edu.tw	smtp:[mail.cis.nctu.edu.tw]
example.com	smtp:[192.168.23.56]:20025
orillynet.com	smtp
ora.com	maildrop
kdent@ora.com	error:no mail accepted for kdent

# 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`

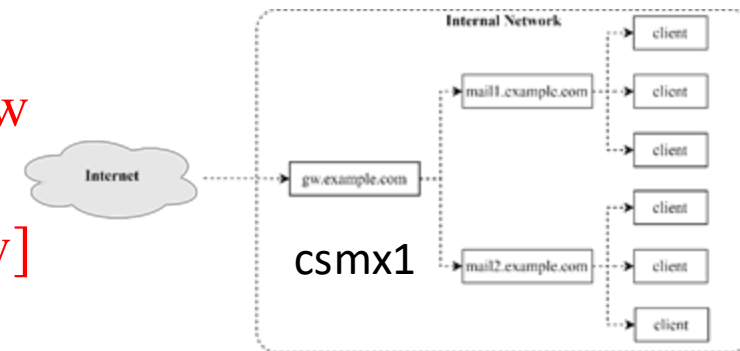
# Mail Relaying – Inbound Mail Gateway (1)

- 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`

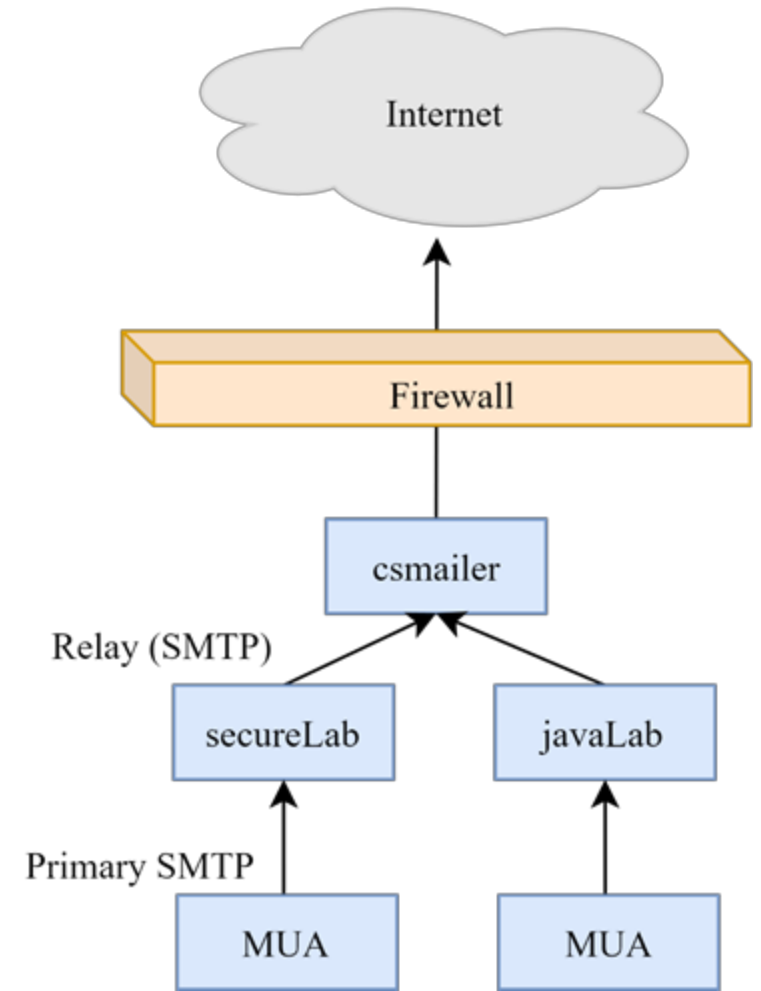


javaLab  
secureLab

# Mail Relaying – Outbound Mail Gateway

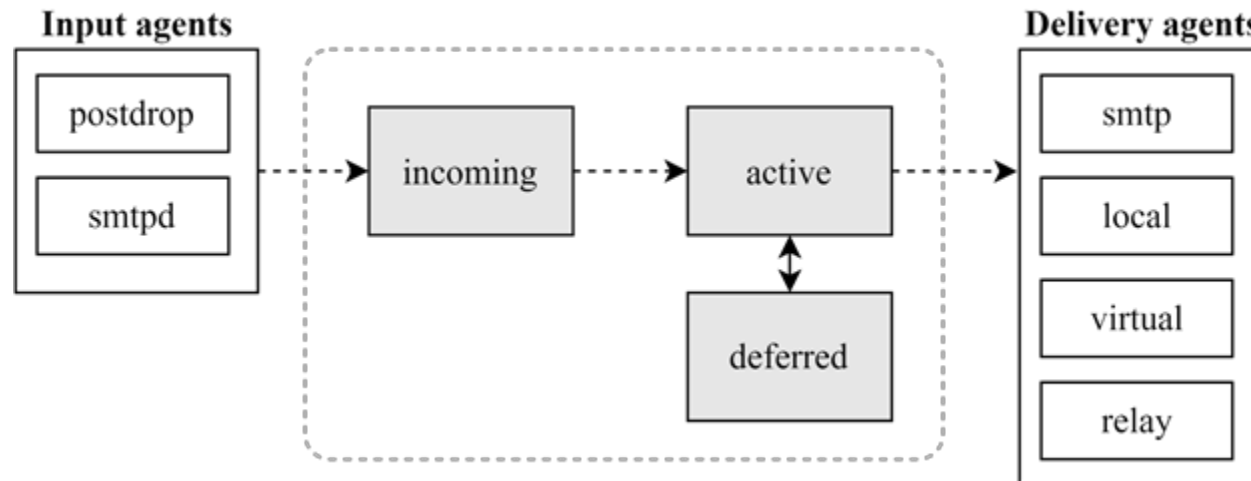
- Outbound Mail Gateway
  - Accept mails from inside network and relay them to Internet hosts
- To be OMG, suppose
  - You are administrator for cs.nctu.edu.tw
  - Hostname is `csmailer.cs.nctu.edu.tw`
  - You have to be the **OMG for secureLab.cs.nctu.edu.tw** and **javaLab.cs.nctu.edu.tw**
- 1. In `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
  - Takes messages alternatively between **incoming and deferred to active** queue



# Queue Management – Queue Scheduling

- Double delay in deferred messages
  - Between
    - `minimal_backoff_time = 300s`
    - `maximal_backoff_time = 4000s`
  - `Periodically scan` deferred queue for reborn messages
    - `queue_run_delay = 300s`
- `Deferred => bounce`
  - `maximal_queue_lifetime = 5d`

# Queue Management – Message Delivery

- Controlling outgoing messages
  - Avoid overwhelming the destination when there are lots of messages to it
  - Concurrent delivery succeed => increase concurrency between:
    - `initial_destination_concurrency = 5`
    - `default_destination_concurrency_limit = 20`
    - Under control by
      - `maxproc` in `/usr/local/etc/postfix/master.cf`
    - Customization for different transport mailers:
      - `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`
    - Customization for transport mailers:
      - `smtp_destination_recipient_limit = 100`

# Queue Management – Error Notification

- Sending error messages to administrator
  - Error classes to be generated and **sent to administrator**
    - notify\_classes = resource, software
  - Possible error classes

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

# Queue Management – Queue Tools (2)

- [postqueue\(1\)](#)

- `postqueue -p` (or “`mailq`”)
  - Show the queued mails (no **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**

- [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

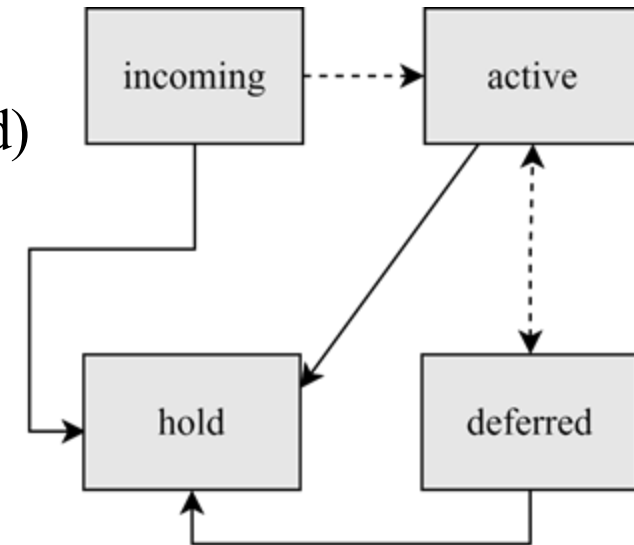
nasa [/home/lctseng] -lctseng- sudo postcat -q 3314234284A
*** ENVELOPE RECORDS deferred/3/3314234284A ***
message_size:                602                214                1                0
602
message arrival time: Sat May 19 04:16:20 2012
create_time: Sat May 19 04:16:20 2012
sender: root@nasa.cs.nctu.edu.tw
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:
...
```

# Queue Management – Queue Tools (1)

- [postsuper\(1\)](#)

- **Delete** queued messages *msg id*
  - `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`



# 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
  - Accept mails for both [canonical and virtual domains](#)
  - 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

- 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** ←

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

- Limitation

- Need to maintain system accounts for virtual domain users

# Multiple Domains – Separate Domains with Virtual Accounts (1)

- Useful when users in virtual domains:
  - No need to login to system
  - Only retrieve mail through POP/IMAP server
- Procedure
  - Modify "virtual\_mailbox\_domains" to let postfix know what mails it should accept
  - 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:
    - 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

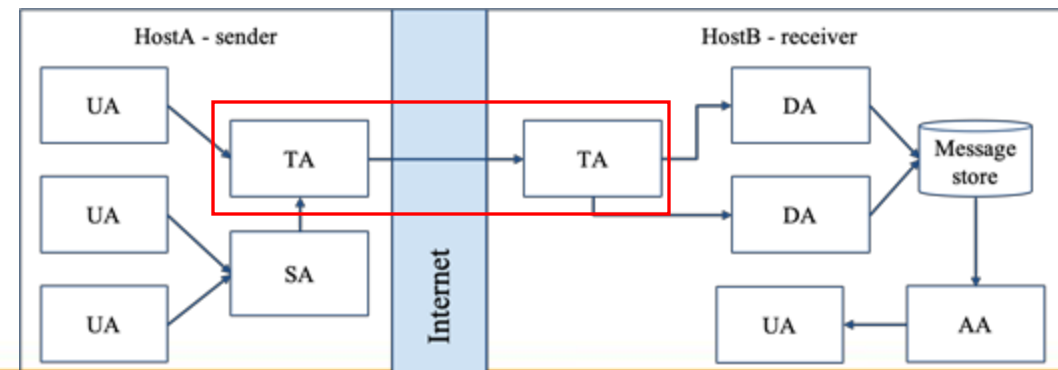
國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

# 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

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

# 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

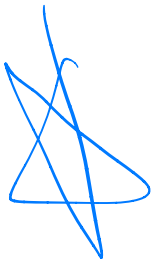
```
sendmail_enable="NONE"
```
    - In /etc/periodic.conf (create if not exists)

```
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
```



In FreeBSD:

Original sendmail: **/usr/sbin/sendmail**

Postfix version: **/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 "mx1.imslab.org"

- Set up these records

- (A record) mx1.imslab.org ⇒ for ip addy

- (A record) imslab.org ⇒ domain

- (MX record) imslab.org

- Points to "mx1.imslab.org"

# Build a basic MTA(4)

- Set up MTA identity
  - In main.cf

```
myhostname = mx1.imslab.org
mydomain = imslab.org
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

```
From tsaimh@nycu.edu.tw Thu May 2 00:21:39 2024
Return-Path: <tsaimh@nycu.edu.tw>
X-Original-To: tsaimh@imslab.org
Delivered-To: tsaimh@imslab.org
Received: from bsd1.imslab.org (localhost
[IPv6:::1])
    by mx1.imslab.org (Postfix) with ESMTMP id
C3ABC1837B
    for <tsaimh@imslab.org>; Thu, 02 May 2024
00:21:16 +0800 (CST)
Subject: This is the subject
Message-Id:
<20240501162121.C3ABC1837B@mx1.imslab.org>
Date: Thu, 02 May 2024 00:21:16 +0800 (CST)
From: tsaimh@nycu.edu.tw
```

This is the body

```
> telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mx1.imslab.org ESMTMP Postfix
ehlo bsd1.imslab.org
250-mx1.imslab.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
mail from: tsaimh@nycu.edu.tw
250 2.1.0 Ok
rcpt to: tsaimh@imslab.org
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: This is the subject

This is the body
.
250 2.0.0 Ok: queued as C3ABC1837B
```

telnet

# Send test mails to verify your MTA(2)

- The "mail" command

mail

```
$ mail -s "test from imslab" tsaimh@nycu.edu.tw  
you have mail  
This is a test mail from bsd1.imslab.org  
regards,  
IMSLab  
EOT          (Press Ctrl+D)
```

Gmail: tsaimh@nycu.edu.tw

test from imslab

外部

收件匣 ×



**Meng-Hsun Tsai** <tsaimh@imslab.org>

寄給我 ▾



翻譯成中文 (繁體)



This is a test mail from [bsd1.imslab.org](https://bsd1.imslab.org)

regards,

IMSLab

# Send test mails to verify your MTA(3)

- Mail source text of the previous example

Delivered-To: [tsaimh@nycu.edu.tw](mailto:tsaimh@nycu.edu.tw)

< ... omitted ... >

Authentication-Results: mx.google.com; spf=neutral (google.com: 140.116.245.245 is neither permitted nor denied by best guess record for domain of [tsaimh@imslab.org](mailto:tsaimh@imslab.org))  
smtp.mailfrom=[tsaimh@imslab.org](mailto:tsaimh@imslab.org)

Received: by [mx1.imslab.org](mailto:mx1.imslab.org) (Postfix, from userid 1001) id E65C81837D; Thu, 02 May 2024 00:41:10 +0800 (CST)

To: [tsaimh@nycu.edu.tw](mailto:tsaimh@nycu.edu.tw)

Subject: test from imslab

Message-Id: <20240501164110.E65C81837D@mx1.imslab.org> Date: Thu, 02 May 2024 00:41:10 +0800 (CST)

From: Meng-Hsun Tsai <[tsaimh@imslab.org](mailto:tsaimh@imslab.org)>

This is a test mail from [bsd1.imslab.org](mailto:bsd1.imslab.org)

regards,  
IMSLab

# 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.nctu.cs.net  
(host csmx3.cs.nctu.edu.tw[140.113.235.119] said: 450 4.1.8  
<lctseng@nasa.lctseng.nctu.cs.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

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

# 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 dem01.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to dem01.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 dem01.nasa.lctseng.nctucs.net ESMTP Postfix
MAIL FROM: lctseng@dem01.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
- References
  - <http://wiki2.dovecot.org/>
  - [http://www.postfix.org/SASL\\_README.html](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 dem01.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to dem01.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 dem01.nasa.lctseng.nctucs.net ESMTP Postfix
EHLO linuxhome.cs.nctu.edu.tw
250-dem01.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 dem01.nasa.lctseng.nctucs.net 25
Trying 140.113.168.238...
Connected to dem01.nasa.lctseng.nctucs.net.
Escape character is '^]'.
220 dem01.nasa.lctseng.nctucs.net ESMTF Postfix
AUTH PLAIN AHR1c3QAdGVzdHBhc3N3b3Jk
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@dem01.nasa.lctseng.nctucs.net>
Date: Mon, 7 Mar 2016 15:01:09 +0800 (CST)
From: lctseng@dem01.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.

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

# 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
  - 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 be 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:

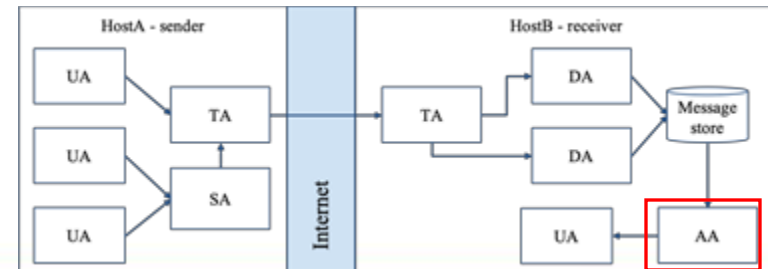
```
openssl s_client -connect host:port
```

- **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

Information Technology 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's 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/](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
- Specify the mail location (must agrees with Postfix)
  - In conf.d/10-mail.conf
- 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

```
first_valid_gid = 0
```

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

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

# MAA for POP3 and IMAP (3)

- After restarting 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://it.cs.nycu.edu.tw/mail-receive>