

The image features a decorative design on the left side consisting of three overlapping blue squares of varying sizes. A solid dark blue horizontal line extends from the right edge of the middle square across the width of the slide.

Postfix

Postfix

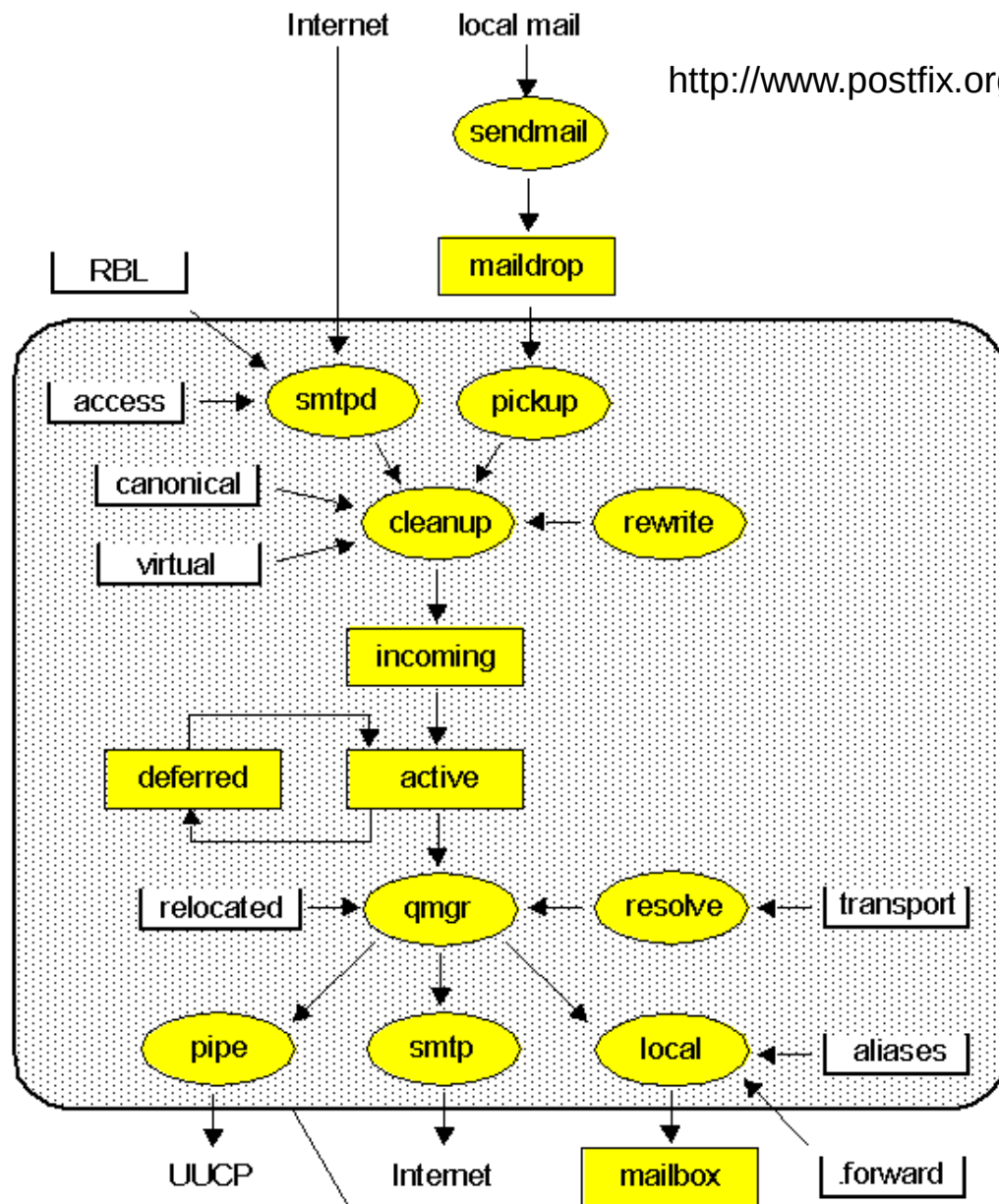
❑ Free and open source mail transfer agent (MTA)

- For the routing and delivery of email
- Intended as a fast, easy-to-administer, and secure alternative to the widely-used Sendmail
- Formerly VMailer / IBM Secure Mailer
 - By Wietse Venema at the IBM Thomas J. Watson Research Center
- IBM Public License

❑ First released in mid-1999

❑ <http://www.postfix.org>

- <http://www.postfix.org/documentation.html>



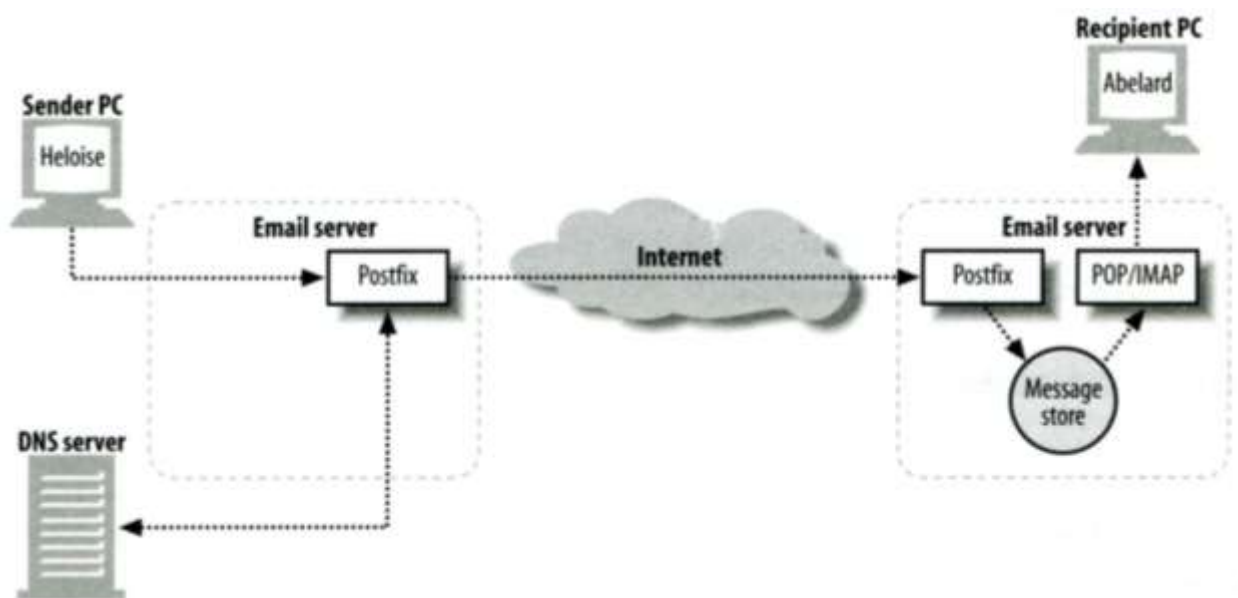
- Mail Programs
- Mail Queues or Files
- Lookup Tables

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

Role of Postfix

❑ MTA that

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



Postfix Architecture

❑ Modular-design MTA

- Not like sendmail of monolithic system
- Decompose into several individual program that each one handle specific task
- The most important daemon: `master` daemon
 - Reside in memory
 - Get configuration information from `master.cf` and `main.cf`
 - Invoke other process to do jobs

❑ Major tasks

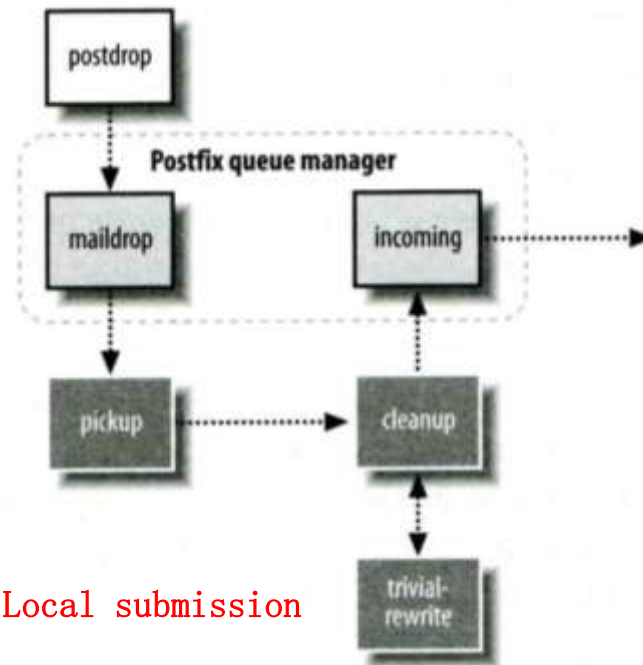
- Receive mail and put in queue
- Queue management
- Delivery mail from queue



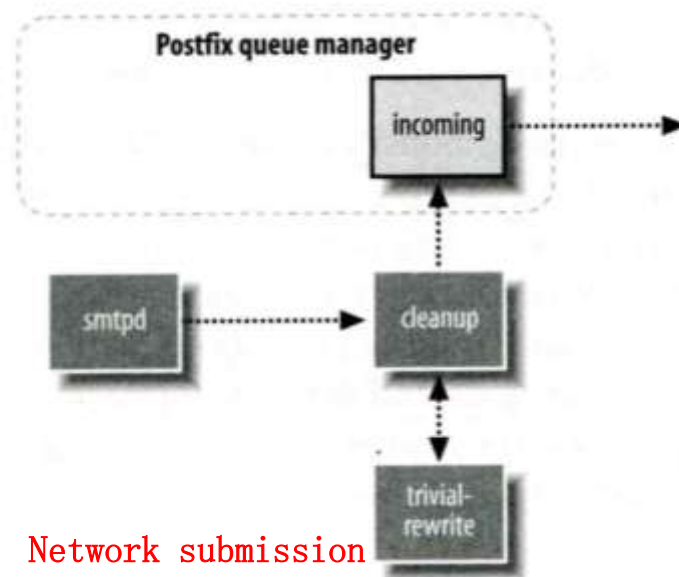
Postfix Architecture – Message IN

❑ Four ways

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



Local submission



Network submission

Postfix Architecture – Queue

❑ Five different queues

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

Postfix Architecture – Message OUT (1)

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

Postfix Architecture –

Message OUT (2)

❑ Other delivery agent (MDA)

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

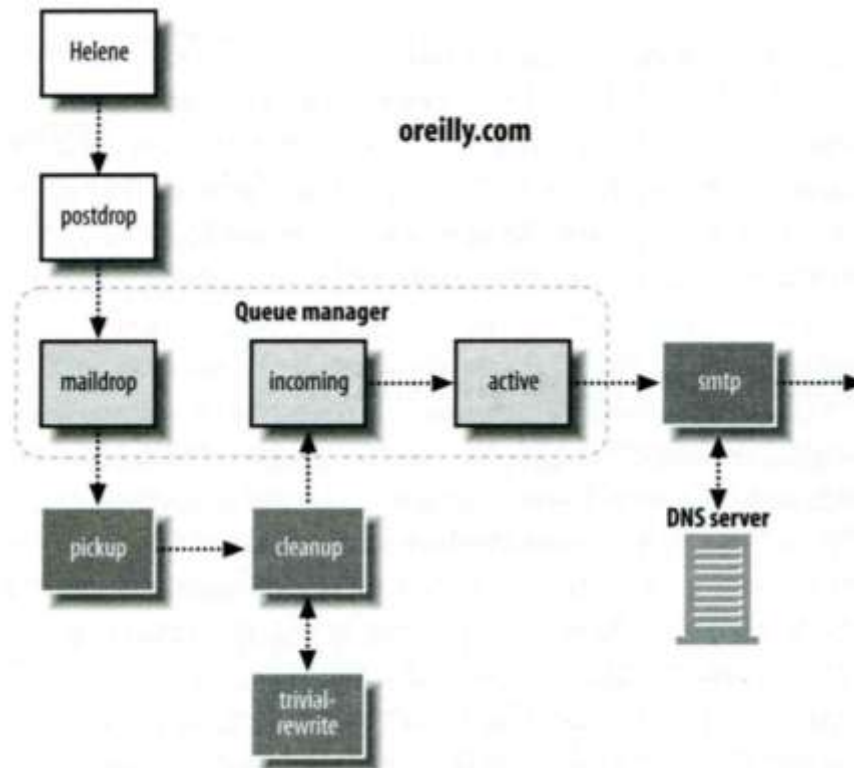
pickup	fifo	n	–	n	60	1	pickup
cleanup	unix	n	–	n	–	0	cleanup
bounce	unix	–	–	n	–	0	bounce
defer	unix	–	–	n	–	0	bounce
smtp	unix	–	–	n	–	–	smtp
relay	unix	–	–	n	–	–	smtp

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

Message Flow in Postfix (1)

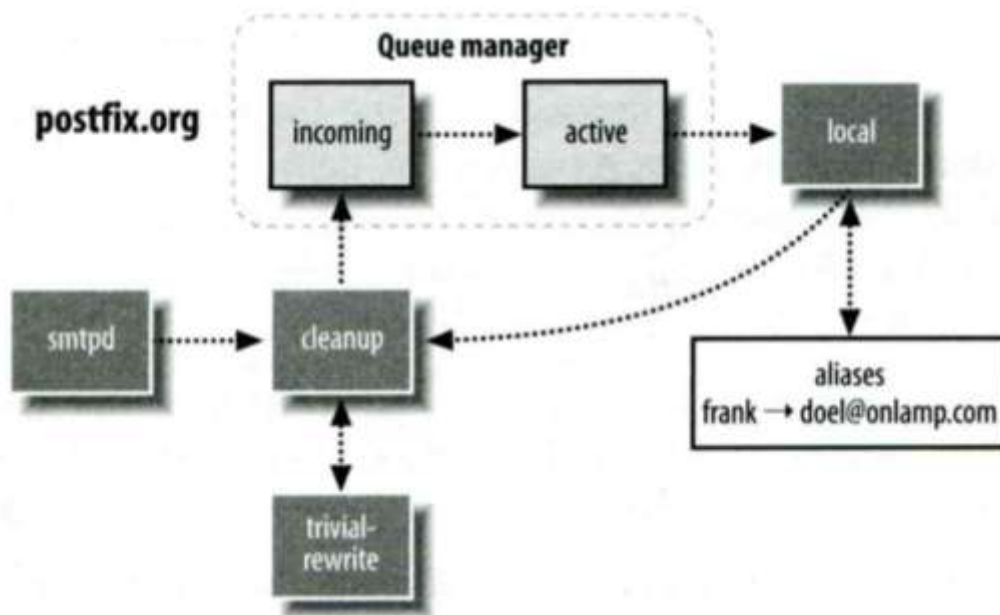
□ Example

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



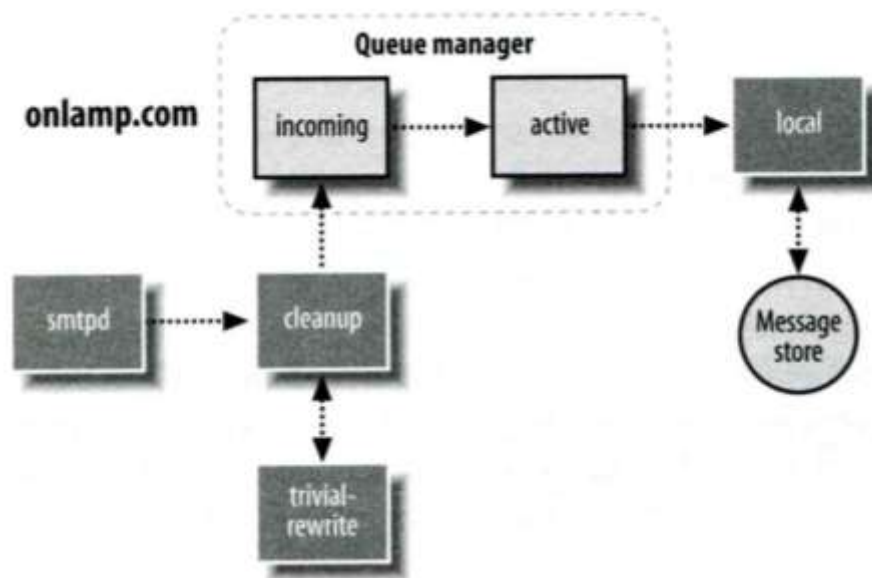
Message Flow in Postfix (2)

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



Message Flow in Postfix (3)

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



Message Store Format

❑ The Mbox format

- Store messages in single file for each user
- Each message start with “From ” line and continued with message headers and body
- Mbox format has file-locking problem

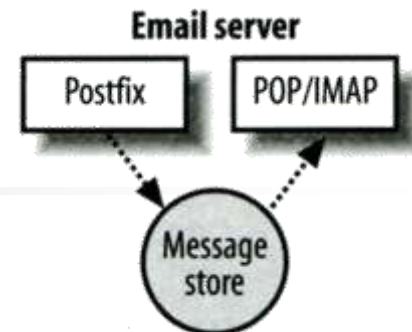
❑ The Maildir format

- Use structure of directories to store email messages
- Each message is in its owned file
- Three subdirectories
 - cur, new and tmp
- Maildir format has scalability problem
 - Quick in locating and deleting

❑ Related parameters (in main.cf)

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

Postfix and POP/IMAP

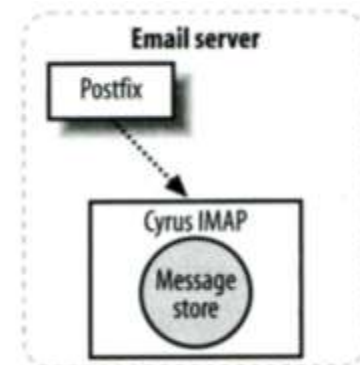


❑ POP vs. IMAP

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

❑ Cooperation between Postfix and POP/IMAP

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



Postfix Configuration

❑ Two most important configuration files

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

❑ Edit configuration file

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

❑ Reload postfix whenever there is a change

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

Postfix Configuration – Lookup tables (1)

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

Postfix Configuration – Lookup tables (2)

- ❑ Database format
 - `% postconf -m`
 - List all available database format
 - `% postconf default_database_type`
- ❑ Use databased-lookup table in `main.cf`
 - syntax
 - Parameter = type:name
 - Ex:
`check_client_access = hash:/etc/access`

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

Postfix Configuration – Lookup tables (3)

❑ Regular expression tables

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

Postfix Configuration – system-wide aliases files

- ❑ Using aliases in Postfix
 - `alias_maps = hash:/etc/aliases`
 - `alias_maps = hash:/etc/aliases, nis:mail.aliases`
 - `alias_database = hash:/etc/aliases`
 - Tell `newaliases` command which aliases file to build
- ❑ To Build alias database file
 - `% postalias /etc/aliases`
- ❑ Alias file format (same as sendmail)
 - RHS can be
 - Email address, filename, |command, :include:
- ❑ Alias restriction
 - `allow_mail_to_commands = alias, forward`
 - `allow_mail_to_files = alias, forward`

Postfix Configuration – MTA Identity

❑ Four related parameters

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

Postfix Configuration – Relay Control (1)

❑ Open relay

- A mail server that permit anyone to relay mails
- By default, postfix is not an open relay

❑ A mail server should

- Relay mail for trusted user
 - Such as smtp.cs.nctu.edu.tw
- Relay mail for trusted domain
 - Such as smtp.csie.nctu.edu.tw trust nctu.edu.tw

Postfix Configuration – Relay Control (2)

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

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

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

Postfix Configuration – master.cf (1)

❑ /usr/local/etc/postfix/master.cf

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

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

Postfix Configuration – master.cf (2)

❑ Configuration options

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

Postfix Configuration – master.cf (3)

- chroot
 - chroot location is defined in “queue_directory”
- wakeup
 - Periodic wake up to do jobs, such as pickup daemon
- maxproc
 - Number of processes that can be invoked simultaneously
 - Default count is defined in “default_process_limit”
- command + args
 - Default path is defined in “daemon_directory”
 - /usr/libexec/postfix

Postfix Configuration – Receiving limits

❑ Enforce limits on incoming mail

- The number of recipients for single delivery
 - `smtpd_recipient_limit = 1000`
- Message size
 - `message_size_limit = 10240000`
- The number of errors before breaking off communication
 - Postfix keep a counter of errors for each client and increase delay time once there is error
 - `smtpd_error_sleep_time = 1s`
 - `smtpd_soft_error_limit = 10`
 - `smtpd_hard_error_limit = 20`

Postfix Configuration – Rewriting address (1)

❑ For unqualified address

- To append “myorigin” to local name.
 - `append_at_myorigin = yes`
- To append “mydomain” to address that contain only host.
 - `append_dot_mydomain = yes`

❑ Masquerading hostname

- Hide the names of internal hosts to make all addresses appear as if they come from the mail gateway
- It is often used in out-going mail gateway
 - `masquerade_domains = cs.nctu.edu.tw`
 - `masquerade_domains = !chairman.cs.nctu.edu.tw cs.nctu.edu.tw`
 - `masquerade_exceptions = admin, root`
- Rewrite to all envelope and header address excepts envelope recipient address
 - `masquerade_class = envelope_sender, header_sender, header_recipient`

Postfix Configuration – Rewriting address (2)

❑ Canonical address

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

chwong@cs.nctu.edu.tw	chwong.NETADM@cs.nctu.edu.tw
chwong@cs.nctu.edu.tw	chwong@nabsd.cs.nctu.edu.tw
- Similar maps
 - sender_canonical_maps
 - recipient_canonical_maps

Postfix Configuration – Rewriting address (3)

❑ Relocated users

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

`@nabsd.cs.nctu.edu.tw` `chbsd.cs.nctu.edu.tw`
`andy@nabsd.cs.nctu.edu.tw` `andyliu@abc.com`

❑ Unknown users

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

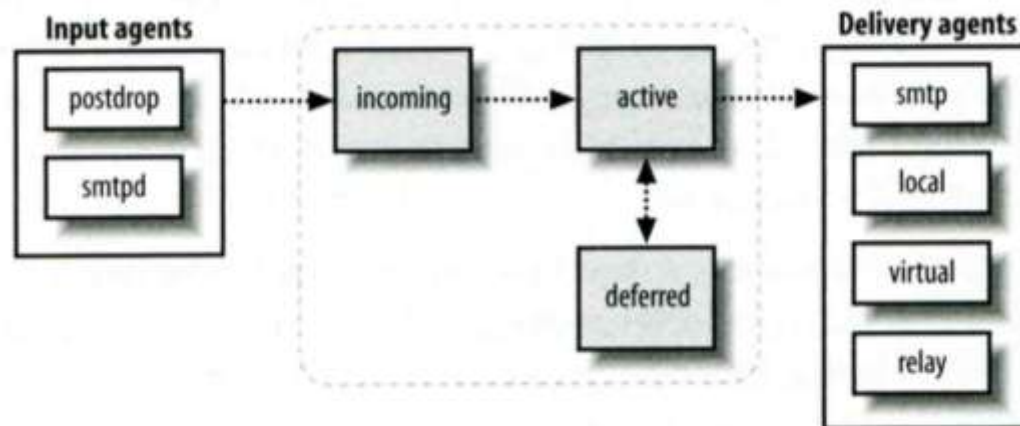
Queue Management

❑ The queue manage daemon

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

❑ Message movement between queues

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



Queue Management – Queue Scheduling

❑ Double delay in deferred messages

- Between
 - `minimal_backoff_time` = 1000s
 - `maximal_backoff_time` = 4000s
- `qmgr` daemon periodically scan deferred queue for reborn messages
 - `queue_run_delay` = 1000s

❑ Deferred → bounce

- `maximal_queue_lifetime` = 5d

Queue Management – Message Delivery

❑ Controlling outgoing messages

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

Queue Management – Error Notification

❑ Sending error messages to administrator

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

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

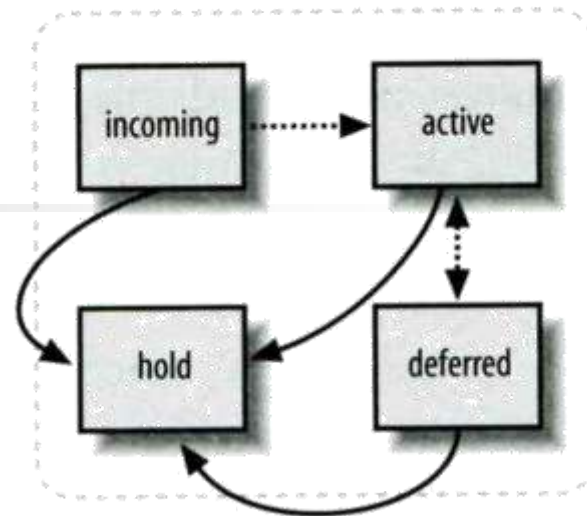
Queue Management – Queue Tools (1)

❑ postfixqueue command

- postfixqueue -p
 - Generate sendmail mailq output
- postfixqueue -f
 - Attempt to deliver all queued mail
- postfixqueue -s cs.nctu.edu.tw
 - Schedule immediate delivery of all mail queued for site

❑ postsuper command

- postsuper -d DBA3F1A9 (from incoming, active, deferred, hold)
- postsuper -d ALL
 - Delete queued messages
- postsuper -h DBA3F1A9 (from incoming, active, deferred)
- postsuper -h ALL
 - Put messages "on hold" so that no attempt is made to deliver it
- postsuper -H DBA3F1A9
- postsuper -H ALL
 - Release messages in hold queue
- postsuper -r DBA3F1A9
- postsuper -r ALL
 - Requeue messages into maildrop queue



Queue Management – Queue Tools (2)

❑ postcat

- Display the contents of a queue file

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

```
-- 0 Kbytes in 1 Request.
```

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

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

Mail Relaying – Transport Maps (1)

❑ Transport maps

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

`domain_or_address transport:nexthop`

`csie.nctu.edu.tw smtp:[mailgate.csie.nctu.edu.tw]`

`cs.nctu.edu.tw smtp:[csmailgate.cs.nctu.edu.tw]`

`cis.nctu.edu.tw smtp:[mail.cis.nctu.edu.tw]`

`example.com smtp:[192.168.23.56]:20025`

`orillynet.com smtp`

`ora.com maildrop`

`kdent@ora.com error:no mail accepted for kdent`

Mail Relaying – Transport Maps (2)

- ❑ One usage in transport map
 - Postponing mail relay
 - Such as ISP has to postpone until customer network is online
 - Ex:
 - I am an ISP, and I has a mail server that is MX for abc.com

```
In /usr/local/etc/postfix/transport
abc.com    ondemand
```

```
In /usr/local/etc/postfix/master.cf
ondemand  unix  -  -  n  -  -  smtp
```

```
In /usr/local/etc/postfix/main.cf
defer_transports = ondemand
transport_maps = hash:/usr/local/etc/postfix/transport
```

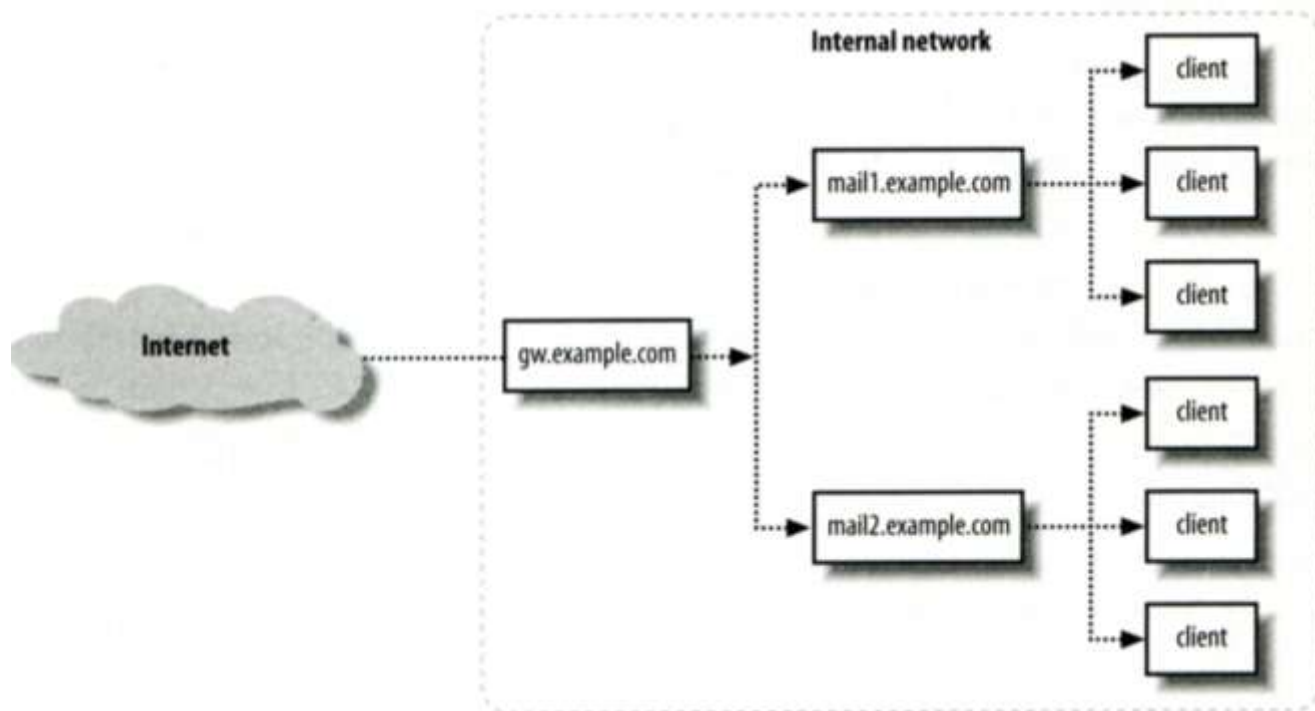
Whenever the customer network is online, do

```
$ postqueue -f abc.com
```

Mail Relaying – Inbound Mail Gateway (1)

❑ Inbound Mail Gateway

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



Mail Relaying – Inbound Mail Gateway (2)

❑ To be IMG, suppose

- You are administrator for cs.nctu.edu.tw
 - You have to be the IMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw
1. The MX record for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw should point to csmx1.cs.nctu.edu.tw
 2. In csmx1.cs.nctu.edu.tw,
relay_domains = secureLab.cs.nctu.edu.tw javaLab.cs.nctu.edu.tw
transport_maps = hash:/usr/local/etc/postfix/transport
secureLab.cs.nctu.edu.tw relay:[secureLab.cs.nctu.edu.tw]
javaLab.cs.nctu.edu.tw relay:[javaLab.cs.nctu.edu.tw]
 3. In secureLab.cs.nctu.edu.tw (and so do javaLab.cs.nctu.edu.tw)
mydestination = secureLab.cs.nctu.edu.tw

Mail Relaying – Outbound Mail Gateway

- ❑ Outbound Mail Gateway
 - Accept mails from inside network and relay them to Internet hosts on behalf of internal mail servers
 - ❑ To be OMG, suppose
 - You are administrator for cs.nctu.edu.tw
 - You have to be the OMG for secureLab.cs.nctu.edu.tw and javaLab.cs.nctu.edu.tw
1. In csmailer.cs.nctu.edu.tw
mynetworks = hash:/usr/local/etc/postfix/mynetworks
secureLab.cs.nctu.edu.tw
javaLab.cs.nctu.edu.tw
 2. All students in secureLab/javaLab will configure there MUA (ex. outlook) to use secureLab/javaLab.cs.nctu.edu.tw to be the SMTP server
 3. In secureLab/javaLab.cs.nctu.edu.tw,
relayhost = [csmailer.cs.nctu.edu.tw]

Advanced Aliasing – Virtual Alias Maps

□ Virtual Alias Map

- It rewrites recipient addresses for all local, all virtual, and all remote mail **destinations**.
- `virtual_alias_maps = hash:/usr/local/etc/postfix/virtual`
- Ex:

src-address

chwong@csie.nctu.edu.tw

@csie.nctu.edu.tw

chwong

dst-address

@chbsd.cs.nctu.edu.tw

@cs.nctu.edu.tw

ch0nsi@gmail.com

- Applying regular expression

➤ `virtual_alias_maps = pcre:/usr/local/etc/postfix/virtual`

`/chwong@csie\.nctu\.edu\.tw/`

`@chbsd.cs.nctu.edu.tw`

`/@csie\.nctu\.edu\.tw/`

`@cs.nctu.edu.tw`

`/(\S+)\.(\S+)\@nabsd\.cs\.nctu\.edu\.tw/ $1@nabsd.cs.nctu.edu.tw`

Multiple Domains

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

Multiple Domains –

Shared Domain with System Account

❑ Situation

- The mail system should accept mails for both canonical and virtual domains and
- The same mailbox for the same user id

❑ Procedure

- Modify “mydomain” to canonical domain
- Modify “mydestination” parameter to let mails to virtual domain can be local delivered
- Ex:
 - mydomain = cs.nctu.edu.tw
 - mydestination = \$myhostname, \$mydomain, csie.nctu.edu.tw

※ In this way, mail to both chwong@cs.nctu.edu.tw and chwong@csie.nctu.edu.tw will go to csmailgate:/var/mail/chwong

❑ Limitation

- Can not separate chwong@cs.nctu.edu.tw from chwong@csie.nctu.edu.tw

Multiple Domains –

Separate Domains with System Accounts

❑ Situation

- The mail system should accept mails for both canonical and virtual domains and
- Mailboxes are not necessarily the same for the same user id

❑ Procedure

- Modify “mydomain” to canonical domain
- Modify “virtual_alias_domains” to accept mails to virtual domains
- Create “virtual_alias_maps” map
- Ex:
 - mydomain = cs.nctu.edu.tw
 - virtual_alias_domains = abc.com.tw, xyz.com.tw
 - virtual_alias_maps = hash:/usr/local/etc/postfix/virtual
 - In /usr/local/etc/postfix/virtual
 - CEO@abc.com.tw andy
 - @xyz.com.tw jack

❑ Limitation

- Need to maintain UNIX account for virtual domain user

Multiple Domains –

Separate Domains with Virtual Accounts (1)

❑ Useful when users in virtual domains:

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

❑ Procedure

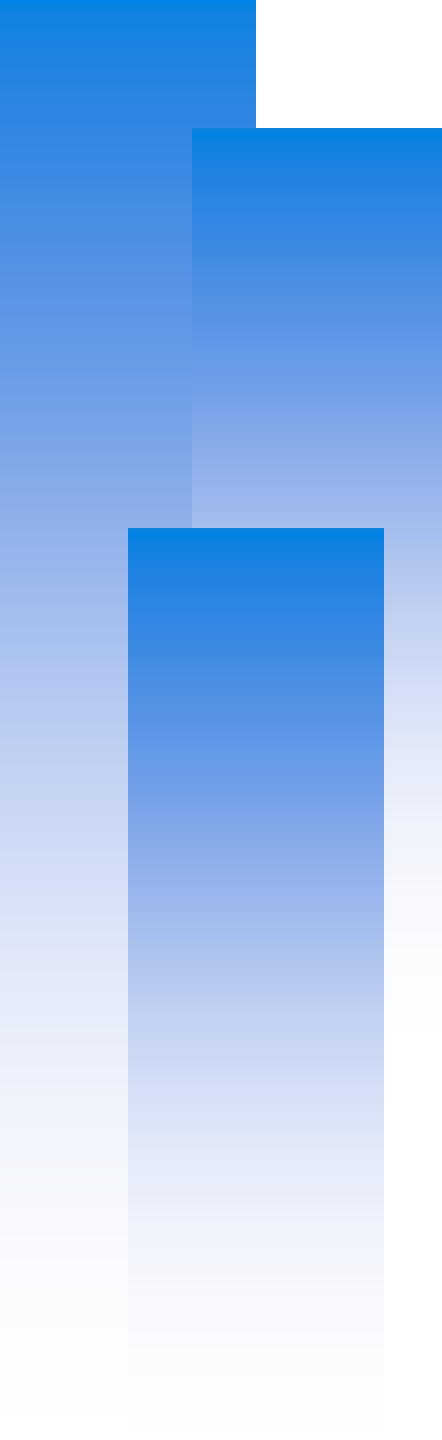
- Modify “virtual_mailbox_domains” to let postfix know what mails it should accepts
- Modify “virtual_mailbox_base” and create related directory to put mails
- Create “virtual_mailbox_maps” map
- Ex:
 - virtual_mailbox_domain = abc.com.tw, xyz.com.tw
 - virtual_mailbox_base = /var/vmail
 - Create /var/vmail/abc-domain 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
 - Ex:
 - virtual_uid_maps = static:1003
 - virtual_gid_maps = static:105
 - virtual_uid_maps = hash:/usr/local/etc/postfix/virtual_uids
 - virtual_gid_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



Handling Spam in Postfix

Nature of Spam

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

Problems of Spam

❑ Cost

- Waste bandwidth and disk space
- DoS like side-effect
- Waste time and false deletion
- Bounce messages of nonexistent users
 - Nonexistent return address
 - Forged victim return address

❑ Detection

- Aggressive spam policy may cause high false positive

Anti-Spam –

Client-Based Detection (1)

☐ Client-blocking

- Use IP address, hostnames or email address supplied by clients when they connect to send a message
- Compared with Spammer list
- Problems
 - IP address, hostname, email address are forged
 - Innocent victim open relay host

☐ DNSBL (DNS-based Blacklist)

- Maintain large database of systems that are known to be open relays or that have been used for spam

☐ Grey Listing

☐ SPF – Sender Policy Framework

☐ ...

Anti-Spam –

Client-Based Detection (2)

❑ What DNSBL maintainers do

- Suppose csie has a Blacklist DNS database
 - Suppose DNSBL Domain “dnsbl.cs.nctu.edu.tw”
- If 140.112.23.118 is detected as open relay
 - There will be a new entry in cs’s blacklist DB
 - 118.23.112.140.dnsbl.cs.nctu.edu.tw
- When we receive a connection from 140.112.23.118
 - Compose 118.23.112.140.dnsbl.cs.nctu.edu.tw
 - DNS query for this hostname
 - Successful means this IP address is suspicious
 - Failed means ok

❑ Using DNSBL

- Review their service options and policies carefully

Anti-Spam – Content-Based Detection

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

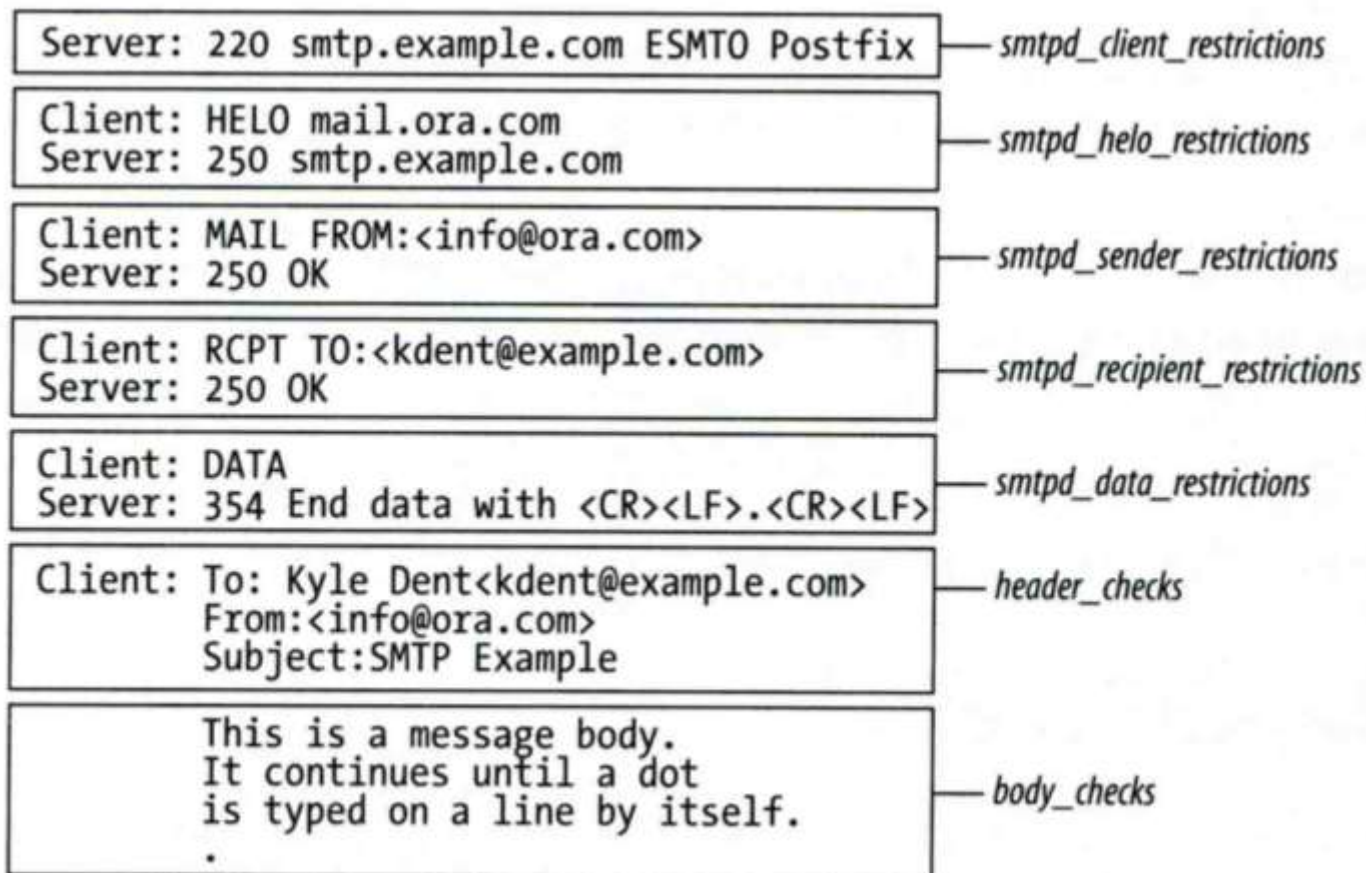
Anti-Spam – Action

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

Postfix Anti-Spam configuration

❑ The SMTP Conversation

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



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

❑ Four rules in relative detection position

- Rules and their default values
 - smtpd_client_restrictions =
 - smtpd_helo_restrictions =
 - smtpd_sender_restrictions =
 - smtpd_recipient_restrictions =
permit_mynetworks, reject_unauth_destination
- Each restriction check result can be:
 - OK (Accept in this restriction)
 - REJECT (Reject immediately without further check)
 - DUNNO (do next check)
- There are 5 types of restrictions

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

1. Access maps

- List of IP addresses, hostnames, email addresses
- Can be used in:

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

smtpd_helo_restrictions = **check_helo_access** hash:/usr/local/etc/postfix/helohost

smtpd_sender_restrictions = **check_sender_access** hash:/usr/local/etc/postfix/sender_access

smtpd_recipient_restrictions = **check_recipient_access** hash:/usr/local/etc/postfix/recipient_access

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

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

- Example of access maps
 - **check_client_access** hash:/etc/access
 - nctu.edu.tw OK
 - 127.0.0.1 OK
 - 61.30.6.207 REJECT
 - **check_helo_access** hash:/postfix/helohost
 - greatdeals.example.com REJECT
 - oreillynet.com OK
 - **check_sender_access** hash:/usr/local/etc/postfix/sender_access
 - viagra.com 553 Please contact +886-3-5712121-54707.
 - aaa@ 553 Invalid MAIL FROM
 - sales@ 553 Invalid MAIL FROM
 - hchen@ 553 Invalid MAIL FROM
 - **check_recipient_access** hash:/usr/local/etc/postfix/recipient_access
 - bin@cs.nctu.edu.tw 553 Invalid RCPT TO command
 - ftp@cs.nctu.edu.tw 553 Invalid RCPT TO command
 - man@cs.nctu.edu.tw 553 Invalid RCPT TO command

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

2. Special client-checking restrictions

- `permit_auth_destination`
 - Mostly used in “`smtpd_recipient_restrictions`”
 - Permit request if destination address matches:
 - The postfix system’s final destination setting
 - » `mydestination`, `inet_interfaces`, `virtual_alias_maps`, `virtual_mailbox_maps`
 - The postfix system’s relay domain
 - » `relay_domains`
 - Found → OK, UnFound → DUNNO
- `reject_unauth_destination`
 - Opposite to `permit_auth_destination`
 - Found → REJECT, UnFound → DUNNO
- `permit_mynetworks`
 - Allow a request if interest IP match any address in “`mynetworks`”
 - Used in `smtpd_recipient_restrictions`
 - Used in `smtpd_client_restrictions`

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

3. Strict syntax restrictions

- Restrictions that does not conform to RFC
 - reject_invalid_hostname
 - Reject hostname with bad syntax
 - reject_non_fqdn_hostname
 - Reject hostname not in FQDN format
 - reject_non_fqdn_sender
 - reject_non_fqdn_recipient
 - For “MAIL FROM” and “RCPT TO” command respectively

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

4. DNS restrictions

- > Make sure that clients and email envelope addresses have valid DNS information
- > reject_unknown_client
 - > Reject if the client IP has no DNS PTR record
 - 215.17.113.140 IN PTR nabsd.cs.nctu.edu.tw.
- > reject_unknown_hostname
 - > Reject if EHLO hostname has no DNS MX or A record
- > reject_unknown_sender_domain
 - > Reject if MAIL FROM domain name has no DNS MX or A record
- > reject_unknown_recipient_domain
 - > Reject if RCPT TO domain name has no DNS MX or A record

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

5. Real-time blacklists

- Check with DNSBL services
- `reject_rbl_client domain.tld`
 - Reject if client IP is detect in DNSBL
- `reject_rhsbl_client domain.tld`
 - Reject if client hostname has an A record under specified domain
- `reject_rhsbl_sender domain.tld`
 - Reject if sender domain in address has an A record under specified domain
- `smtpd_client_restrictions =`
`hash:/etc/access, reject_rbl_client relays.ordb.org`
- `smtpd_sender_restrictions =`
`hash:/usr/local/etc/postfix/sender_access, reject_rhsbl_sender dns.rfc-ignorant.org`

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

6. Policy Service

- Postfix SMTP server sends in a delegated SMTPD access policy request to one special service (policy service).
- Policy service replies actions allowed in Postfix SMTPD access table.
- Usage:
 - `check_policy_service servicename`
- Example: Grey Listing (Using Postgrey)
 - Postgrey daemon runs on port:10023
 - In main.cf:
`smtpd_recipient_restrictions = check_policy_service inet:127.0.0.1:10023`

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

❑smtpd_client_restrictions

- check_client_access
- reject_unknown_client
- permit_mynetworks
- reject_rbl_client
- reject_rhsbl_client

❑smtpd_helo_restrictions

- check_helo_access
- reject_invalid_hostname
- reject_unknown_hostname
- reject_non_fqdn_hostname

❑smtpd_sender_restrictions

- check_sender_access
- reject_unknown_sender_domain
- reject_rhsbl_sender

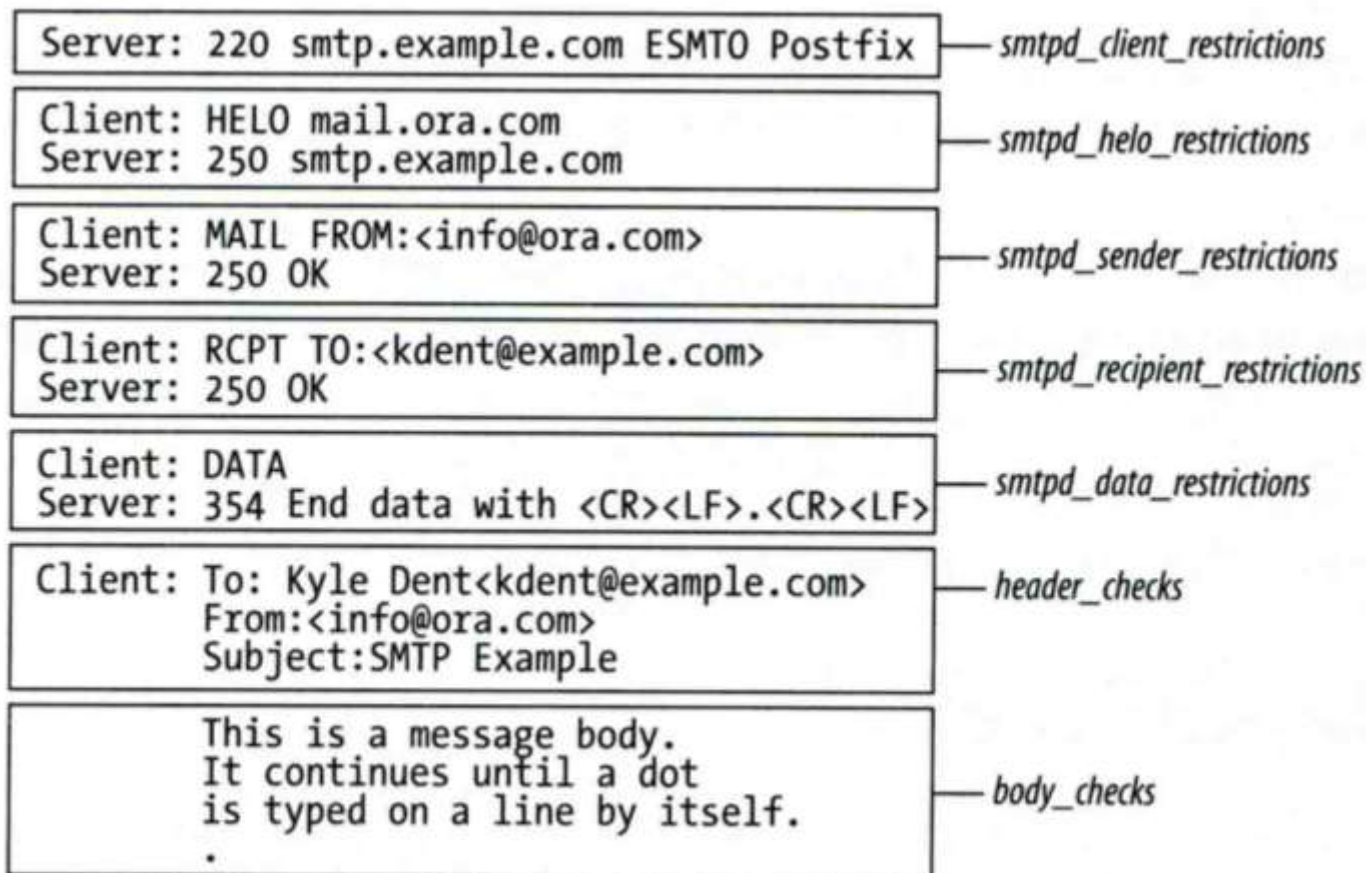
❑smtpd_recipient_restrictions

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

Postfix Anti-Spam configuration

❑ The SMTP Conversation

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



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

❑ 4 rules

- `header_checks`
 - Check for message headers
- `mime_header_checks`
 - Check for MIME headers
- `nested_header_checks`
 - Check for attached message headers
- `body_check`
 - Check for message body

❑ All rules use lookup tables

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

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

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

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

❑ Example of header check

- `header_checks = regexp:/usr/local/etc/postfix/header_checks`
- In `/usr/local/etc/postfix/header_checks`
`/take advantage now/ REJECT`
`/repair your credit/ REJECT`

❑ Example of body check

- `body_checks = regexp:/usr/local/etc/postfix/body_checks`
- In `/usr/local/etc/postfix/body_checks`
`/lowest rates.*\!/ REJECT`
`/[:alpha:]<!--.*-->[:alpha:]/ REJECT`

External Filters

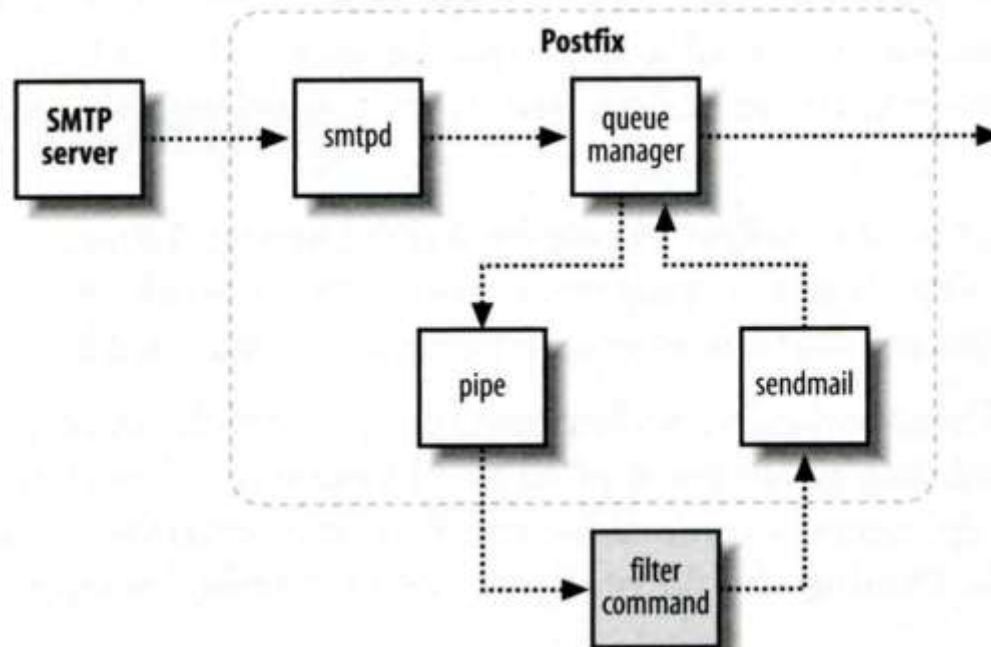
- ❑ Filtering can be done on
 - MTA
 - MDA
 - MUA
 - ✂ Combination of MTA and MUA
 - Adding some extra headers or modifying subject in MTA, and filtering in MUA.

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

Command-Based Filtering (1)

❑ Usage

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



Command-Based Filtering (2)

❑ Configuration

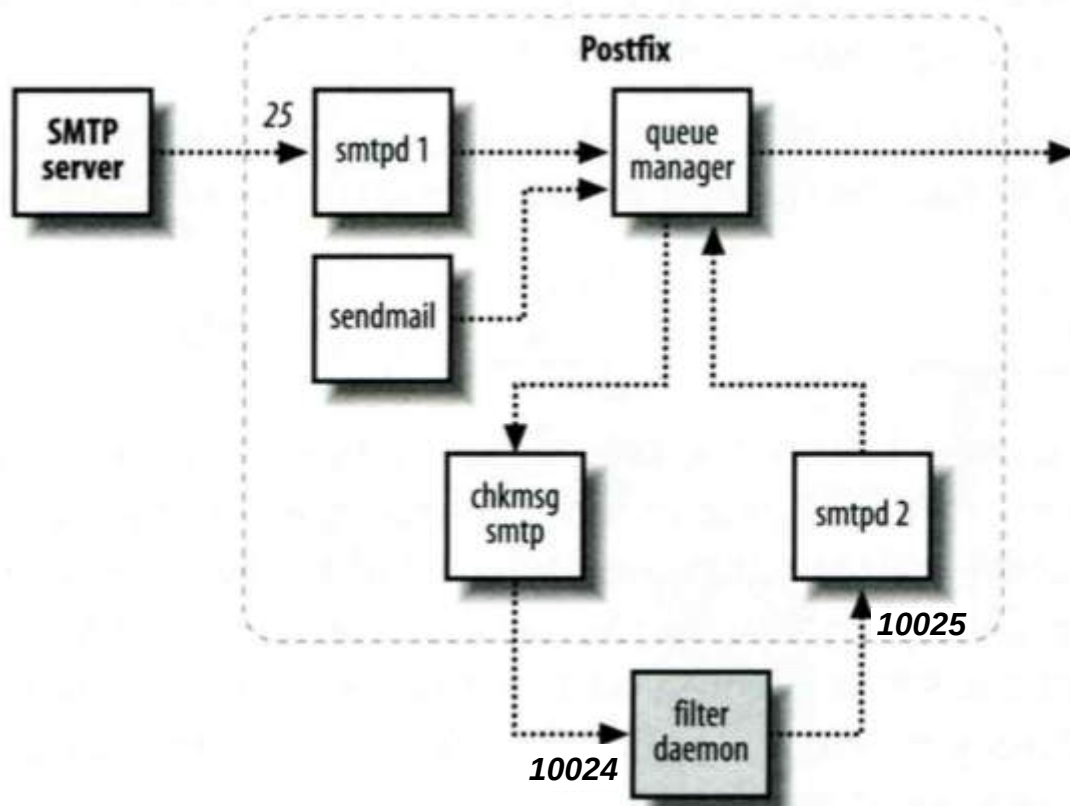
- Prepare your filter program (/usr/local/bin/simple_filt)
- Modify master.cf

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

Daemon-Based Filtering (1)

❑ Usage

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



Daemon-Based Filtering (2)

□ Configuration

- Install and configure your content filter
 - /usr/ports/security/amavisd-new
 - Modify amavisd.conf to send message back
 - \$forward_method = 'smtp:127.0.0.1:10025';
- Edit main.cf to let postfix use filtering daemon
 - content_filter = smtp-amavis:[127.0.0.1]:10024
- Edit master.cf to add two additional services

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


Daemon-Based Filtering (3)

- Anti-virus filtering
 - amavisd-new supports lots of anti-virus scanner
 - Ex:

```
@av_scanners = (

# ['Sophie',
#  \&ask_daemon, ["{} \n", '/var/run/sophie'],
#  qr/(?x)^ 0+ ( : | [\000\r\n]* $)/, qr/(?x)^ 1 ( : | [\000\r\n]* $)/,
#  qr/(?x)^ [-+]? \d+ : (.*) [\000\r\n]* $/ ],
# ['ClamAV-clamd',
#  \&ask_daemon, ["CONTSCAN {} \n", "/var/run/clamav/clamd"],
#  qr/\bOK$/, qr/\bFOUND$/,
#  qr/^.*?: (?!Infected Archive) (.*) FOUND$/ ],

);
```