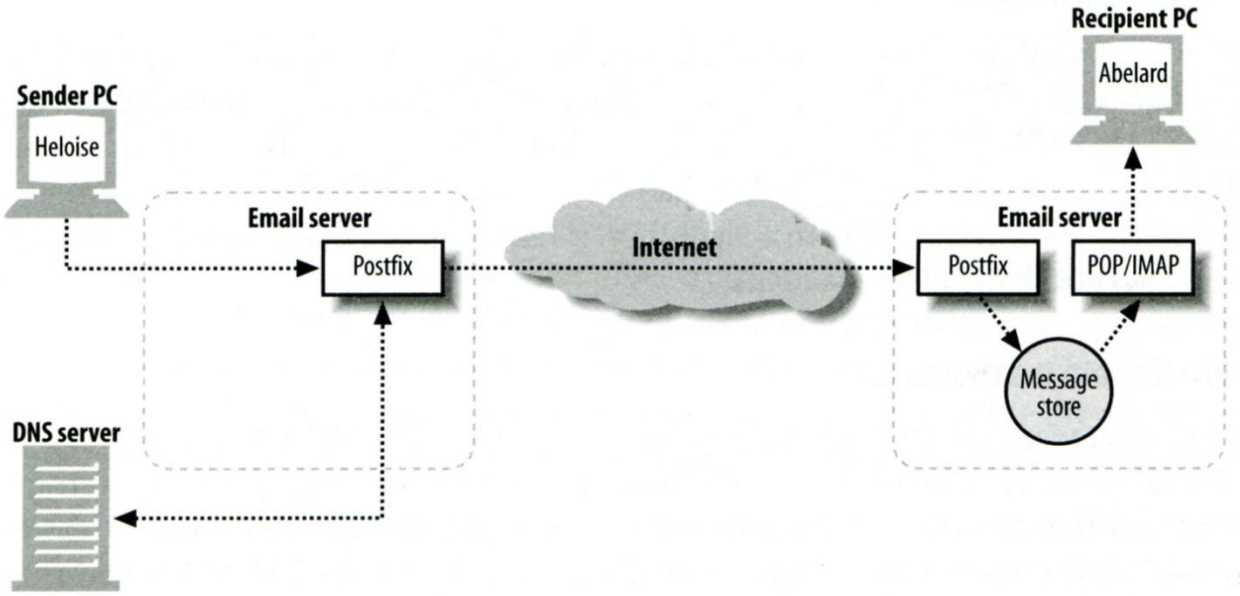
LPIC-2 TRAINING COURSE

Topic 213: Email Services

Role of Postfix

- **MTA that**
  - Receive and deliver email over the network via SMTP
  - Local delivery directly or use other mail de



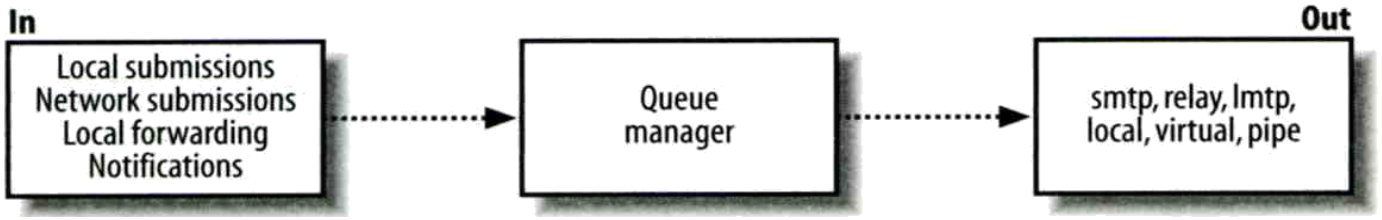
Postfix Architecture

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

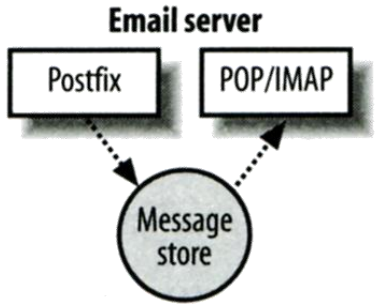
- Receive mail and put in queue
- Queue management
- Delivery mail from queue



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

Postfix and POP/IMAP

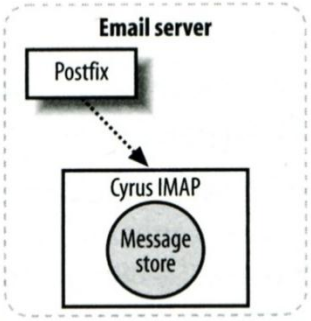


POP vs. IMAP

- 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=mail.ipmac.vn**
    - **# postconf –d myhostname** *#print default setting*
    - **# postconf myhostname** *#print current setting*
- **Reload postfix whenever there is a change**
  - **# postfix reload**

Postfix Configuration – MTA Identity

- **Four related parameters**
  - **myhostname**
    - **myhostname = mail.ipmac.vn**
    - If un-specified, postfix will use '**hostname**' command
  - **mydomain**
    - **mydomain = ipmac.vn**
    - 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**
    - **mydestination = $myhostname, localhost.$mydomain**

Postfix Configuration – Relay Control

- **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
  - Relay mail for trusted domain

Postfix Configuration – Relay Control

- **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
```

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`**

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

AntiSpam: Client-Based Detection

- **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

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

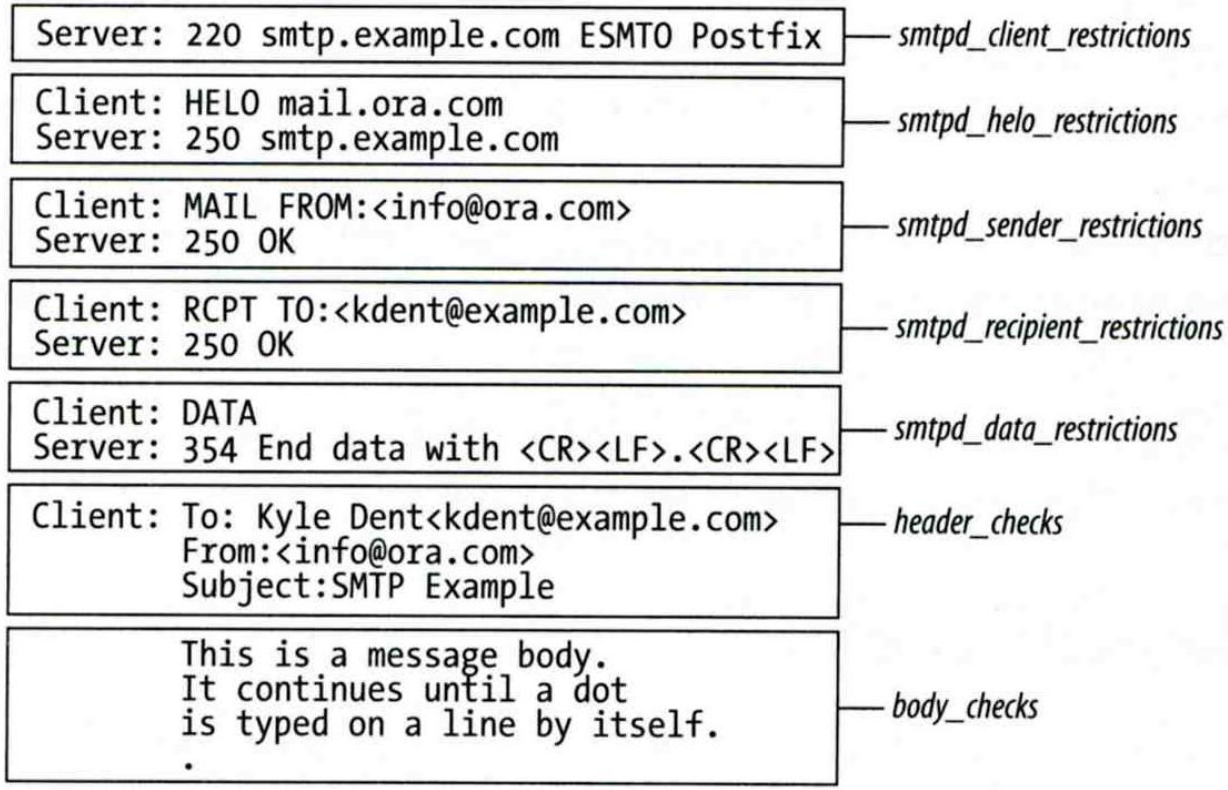
AntiSpam – Action

- **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

Postfix AntiSpam Configuration

The SMTP Conversation

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



Client Detection Rules

- **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

Content-Checking Rules

- **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

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

Thank You !

BACKUP SLIDES