



**sendmail**

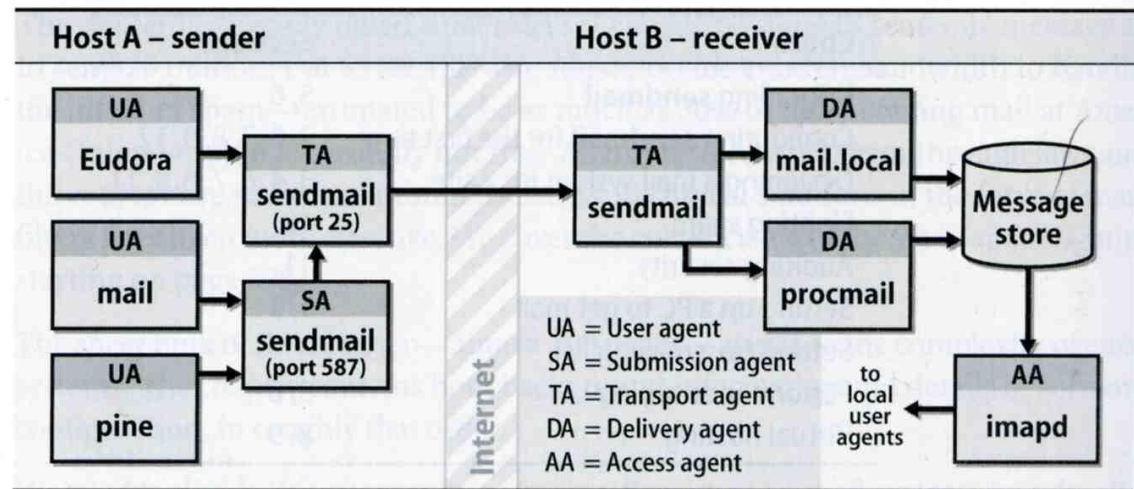


**sendmail.org**

# Introduction

- sendmail is a MTA program
  - The most complete and complex mail transport program with about 70% popularity
  - Interface between MUA and MDA
  - Speak SMTP and deliver mail to remote via the Internet

Exhibit A Mail system components



# History of sendmail

- sendmail version5
  - Eric Allman, student of UC Berkeley, in 1983
- IDA sendmail enhanced from v5
  - Lennart Lovstrand, student of University of Linköping in Sweden, 1987
    - Institutionen for Datavetenskap (cs department)
- KJS sendmail enhanced from IDA
  - Paul Vixie at DECWRL during 1989-1993
    - King James Sendmail
- sendmail version8
  - Eric included enhanced features in IDA and KJS in 1993
- Newest version
  - Sendmail 8.14.2 on 2007-11-01

# Version of sendmail

## o Check your sendmail version

- % /usr/sbin/sendmail -d0.1 -bt < /dev/null
- % telnet localhost 25

```
lucky7 :~ -lwshsu- sendmail -d0.1 -bt < /dev/null
Version 8.14.3
Compiled with: DNSMAP LOG MAP REGEX MATCHGECOS MILTER MIME7T08 MIME8T07
              NAMED BIND NETINET NETINET6 NETUNIX NEWDB NIS PIPELINING SCANF
              STARTTLS TCPWRAPPERS USERDB XDEBUG

===== SYSTEM IDENTITY (after readcf) =====
  (short domain name) $w = lucky7
 (canonical domain name) $j = lucky7.cs.nctu.edu.tw
   (subdomain name) $m = cs.nctu.edu.tw
    (node name) $k = lucky7
=====
```

```
lucky7:~ -lwshsu- telnet localhost 25
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 lucky7.cs.nctu.edu.tw ESMTP Sendmail 8.14.3/8.14.3; Wed, 15 Apr 2009 17:04:22 +0800 (CST)
quit
221 2.0.0 lucky7.cs.nctu.edu.tw closing connection
Connection closed by foreign host.
```

# Major components of sendmail

- /usr/sbin/sendmail
    - The sendmail binary with access mode 4755 setuid to root
  - /etc/mail/sendmail.cf
    - Configuration file
  - /var/spool/mqueue
    - Mail queue directory, with mode 700 owned by root
  - newaliases, mailq, hoststat, ...
    - Various link to sendmail
  - mail.local and smrsh
    - sendmail's safer local delivery agent
- ※ If you want to replace your sendmail with new one
- Install from /usr/ports/mail/sendmail

# Modes of operation

- sendmail can be run in several modes

Flag	Meaning	link
-bd	In daemon mode, on port 25	
-bD	In daemon mode, on port 25, foreground	
-bh	View recent connection information	hoststat
-bH	Purge disk copy of outdated connection info	purgestat
-bi	Initialize hashed aliases	newaliases
-bp	Print mail queue	mailq
-bt	Enter address test mode	
-bv	Verify mail address only; don't send mail	
-bs	Enter SMTP server mode (on stdin, not port 25)	

# Modes of operation

## – daemon mode

### ○ Daemon mode

- sendmail listens on port 25 and waits for work
- Usually specify the `-q` flag to set the interval to process mails in queue
  - `-q30m` to check the queue every 30 minutes
  - `-q1h` to check the queue every 1 hour
- `/var/run/sendmail.pid`
  - Contain the sendmail pid and command that starts it
- Reset sendmail when you change the configuration
  - `# kill -1 `head -1 /var/run/sendmail.pid``
  - `# cd /etc/mail && make restart`

```
lucky7:~ -lwhsu- sudo cat /var/run/sendmail.pid
2034
/usr/sbin/sendmail -L sm-mta -bd -q30m -ODaemonPortOptions=Addr=localhost
```

# Mail queue (1)

- When to store message in queue
  - Messages that host is too busy to deliver immediately or
  - Messages that destination host is unavailable
- Components of each queued message
  - Each message is saved in pieces in several different files
    - Filename: Two-bit-prefix + random-ID

```
lwbsd [/var/spool/mqueue] -lwsu- ls -l
total 4
-rw----- 1 root daemon 8 Apr 24 21:53 dfl30DrYjL039757
-rw----- 1 root daemon 965 Apr 24 21:53 qfl30DrYjL039757
lwbsd [/var/spool/mqueue] -lwsu- sudo mailq
/var/spool/mqueue (1 request)
-----Q-ID----- --Size-- -----Q-Time----- -----Sender/Recipient-----
l30DrYjL039757      8 Tue Apr 24 21:53 <lwbsd@lwbsd.cs.nctu.edu.tw>
                    (Deferred: Operation timed out with nabsd.cs.nctu.edu.tw.)
                    <lwbsd@nabsd.cs.nctu.edu.tw>
Total requests: 1
```



# Mail queue (2)

- Queued message prefix
  - Required pieces
    - qf
      - Message header (H)
      - envelope address
        - Sender Address (S)
        - Recipient Address (R)
      - The date to return as undeliverable
      - Message priority in queue (P)
      - The reason of why being queued (M)
      - Time last processed (K)
      - Time created (T)
    - df
      - Message body

# Mail queue (3)

- Example of qf

```
V8
T1177422814
K1177422889
N1
P30424
MDeferred: Operation timed out with nabsd.cs.nctu.edu.tw.
Fbs
$ localhost [127.0.0.1]
$rESMTP
$slwbsd.cs.nctu.edu.tw
${daemon_flags}
${if_addr}127.0.0.1
S<lw̄hsu@lw̄bsd.cs.nctu.edu.tw>
MDeferred: Operation timed out with nabsd.cs.nctu.edu.tw.
rRFC822; lw̄hsu@nabsd.cs.nctu.edu.tw
RPFD:<lw̄hsu@nabsd.cs.nctu.edu.tw>
```

# Mail queue (4)

```
H??Return-Path: <g>  
H??Received: from lwbsd.cs.nctu.edu.tw (localhost [127.0.0.1])  
    by lwbsd.cs.nctu.edu.tw (8.13.8/8.13.8) with ESMTP id I3ODrYjL039757  
    for <lwhsu@nabsd.cs.nctu.edu.tw>; Tue, 24 Apr 2007 21:53:34 +0800 (CST)  
    (envelope-from lwbsd@lwbsd.cs.nctu.edu.tw)  
H??Full-Name: Li-Wen Hsu  
H??Received: (from lwbsd@localhost)  
    by lwbsd.cs.nctu.edu.tw (8.13.8/8.13.8/Submit) id I3ODrXx9039756  
    for lwbsd@nabsd.cs.nctu.edu.tw; Tue, 24 Apr 2007 21:53:33 +0800 (CST)  
    (envelope-from lwbsd)  
H??Date: Tue, 24 Apr 2007 21:53:33 +0800 (CST)  
H??From: Li-Wen Hsu <lwhsu@lwbsd.cs.nctu.edu.tw>  
H??Message-Id: <200704241353.I3ODrXx9039756@lwbsd.cs.nctu.edu.tw>  
H??To: lwbsd@nabsd.cs.nctu.edu.tw  
H??Subject: From lwbsd to NABSD  
.
```

# Mail queue (5)

- When /var/spool/mqueue is full
  - we can move mqueue to another place and digest it later using this command
    - % /usr/sbin/sendmail -oQ/var/spool/cloggedqueue
- Example script to help to digest large amount of queued mails manually

```
#!/bin/sh
for suffix in 0 1 2 3 4 5 6 7 8 9
do
    mkdir clog${suffix}
    mv ?f*${suffix} clog${suffix}
    /usr/sbin/sendmail -oQclog${suffix}
done
```



# **sendmail Configuration**

# Configuration File (1)

- File path: `/etc/mail/sendmail.cf`
  - Determine how sendmail to do:
    - Choice of delivery agents
    - Address rewriting rules
    - Mail header formats
    - Security precaution
    - Spam resistance
    - Other options
  - Designed to be easy to parse
    - However, it's huge and complex, hard to manipulate it directly.
    - Solution: Use “m4” macro
      - Help to deal with about 98% sendmail.cf configuration cases

# Configuration File (2)

- Problem: Huge & complex, hard to manipulate it directly.
  - Huge size: `%wc -l /etc/mail/sendmail/cf` → 1832 lines
  - Complex: [Part example of sendmail.cf](#)

```
#####  
#   Format of headers   #  
#####  
  
H?P?Return-Path: <$g>  
HReceived: $?sfrom $s $.?$? ($?s$|from $.$_ )  
    $.?{auth_type}{authenticated?{auth_ssf} bits=${auth_ssf}$.)  
    $.by $j ($v/$Z)$?r with $r$. id $i$?{tls_version}  
    (version=${tls_version} cipher=${cipher}bits=${cipher_bits} verify=${verify})$.?$?u  
    for $u; $|;  
    $.b$?g  
    (envelope-from $g)$.  
  
H?D?Resent-Date: $a  
H?D?Date: $a  
H?F?Resent-From: $?x$x <$g>$|$g$.  
H?F?From: $?x$x <$g>$|$g$.  
H?x?Full-Name: $x  
# HPosted-Date: $a  
# H?l?Received-Date: $b  
H?M?Resent-Message-Id: <$t.$i@$j>  
H?M?Message-Id: <$t.$i@$j>
```

# m4 – macro language processor (1)

## o m4 utility

- Front-end preprocessor for other languages
- Transform macros into their corresponding values based on the macro definitions
- Easy example:

```
% cat abc.m
define(`A',`B')
define(`C',`D')
A
C
% m4 abc.m

B
D
```

- Arguments:

- Each argument will be used to replace \$1, \$2 ...

```
% cat argu.m
define(`MYFUNC',`$1$2$3')dnl
MYFUNC(`hello',`-you-',`haha')dnl

% m4 argu.m
hello-you-hahadnl
```



# m4 – macro language processor (2)

## ○ Useful m4 predefined macro

- define # define a new macro
- undefine(arg) # discard a previous “arg” macro definition
- dnl # discard characters up to next newline
- include(arg) # include the “arg” file
- divert(queue) # select an output queue (0 ~ 9)

```
% cat abc.m
define(`A',`B')
define(`C',`D')
A
C
% m4 abc.m

B
D
```

```
% cat abc.m
define(`A',`B')
dnl
define(`C',`D')
dnl
A
C
% m4 abc.m

B
D
```

# Configure with m4 (1)

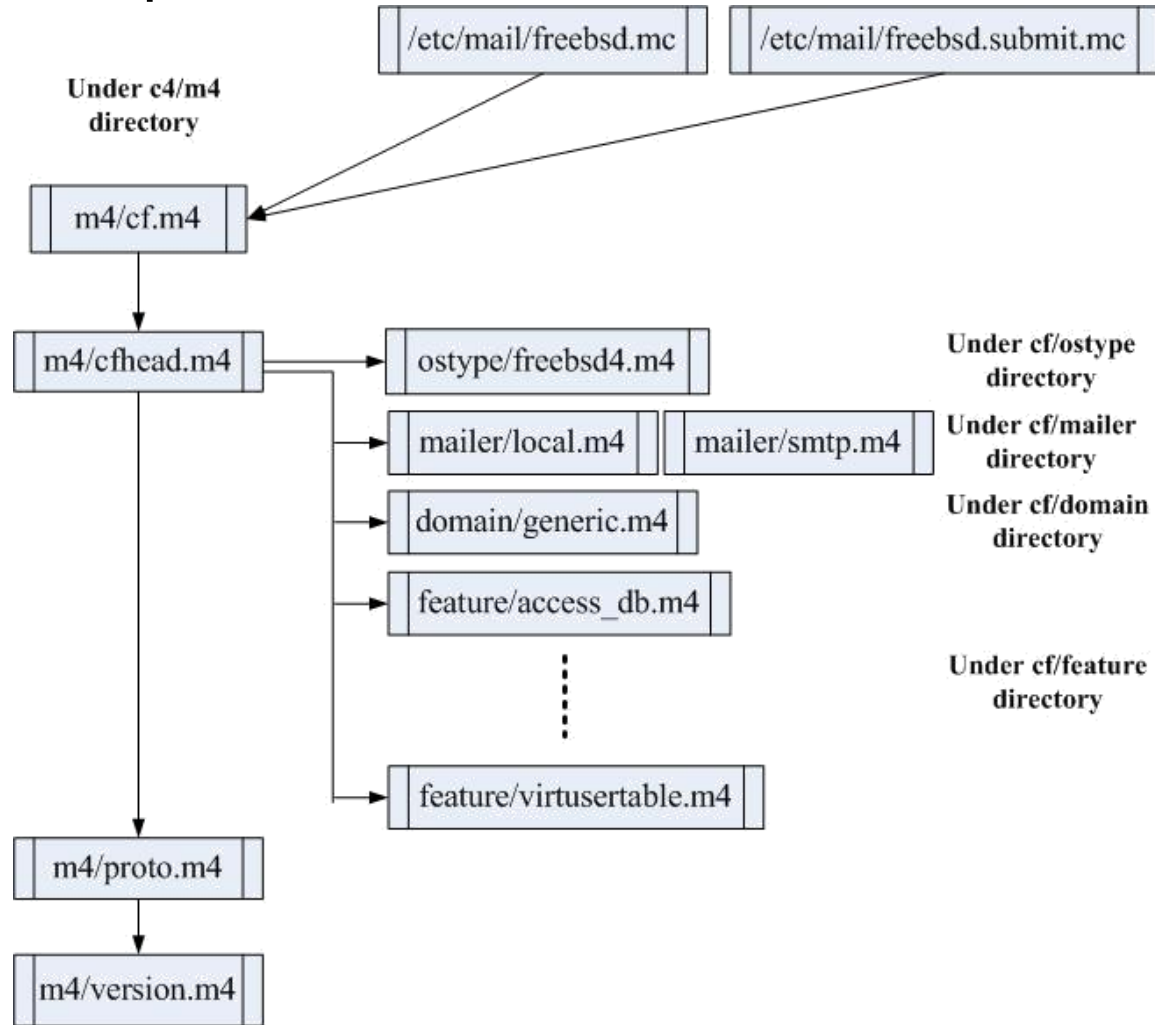
- Generate .cf from .mc file in /etc/mail
  - Edit your mc file (`hostname`.mc) and then
    - % make all
    - % make install
  - mc means “Master Config”
    - A set of m4 macro statements
  - mc will combine with cf.m4 to generate .cf file
  - For example:

```
lwbsd [/etc/mail] -lwshsu- sudo make all
/usr/bin/m4 -D CF_DIR =/usr/share/sendmail/cf/ \
/usr/share/sendmail/cf/m4/cf.m4 lwbsd.mc > lwbsd.cf

/usr/bin/m4 -D CF_DIR =/usr/share/sendmail/cf/ \
/usr/share/sendmail/cf/m4/cf.m4 lwbsd.submit.mc > lwbsd.submit.cf
```

# Configure with m4 (2)

- Relationship between various .mc file



# Configure with m4 (3)

- Convention in sendmail .mc file
  - m4 commands
    - all lower case (ex. define)
  - Predefined macros
    - all capital (ex. OSTYPE)
  - Configurable variable name
    - “conf” + all-capital variable name
    - (ex. confCOPY\_ERROR\_TO)

# Configure with m4 (4)

- Typical order of .mc files

```
divert(-1)
#
# lwbsd:/etc/mail/lwbsd.mc, 2007/04/20
#
divert(0)dnl
VERSIONID(`$FreeBSD: src/etc/sendmail/freebsd.mc,v 1.30.2.2 2006/08/23 03:31:00 gshapiro Exp $')
OSTYPE(`freebsd6')dnl
DOMAIN(`generic')dnl
option definitions
FEATURE(access_db, `hash -o -T<TMPF> /etc/mail/access')
macro definitions
MAILER(local)
MAILER(smtp)
ruleset definitions
```

# Configure with m4 (5)

- Restart sendmail after re-configuration
  - # killall -1 sendmail
    - (or kill -1 `head -1 /var/run/sendmail.pid)
  - # sh /etc/rc.sendmail restart
    - (or /etc/rc.d/sendmail.sh restart)
  - # cd /etc/mail && make restart

# Tables and Databases (1)

- Table
  - A text file that contains information about routing, aliasing, access or others
- Database
  - Hashed version of table
- Database Libraries
  - dbm/ndbm
  - Berkeley DB
- Table → Database conversion
  - Use “makemap” command
  - `% /usr/bin/makemap map-type map.db < map`
  - Map-type
    - dbm use dbm/ndbm hashing algorithm
    - hash use standard DB hashing algorithm
    - btree use DB hashing algorithm with B-tree data structure

# TABLES AND DATABASES (2)

## ○ Tables

- /etc/mail/mailertable
- /etc/mail/genericstable
- /etc/mail/virtusertable
- /etc/mail/access
- /etc/mail/aliases



## ○ Databases

- /etc/mail/mailertable.db
- /etc/mail/genericstable.db
- /etc/mail/virtusertable.db
- /etc/mail/access.db
- /etc/mail/aliases.db





# Macros



# Macros

## – VERSIONID macro

- Embed version information
  - Each config file should put this macro to insert an identifier
  - These identifiers will appear in the final sendmail.cf file as a comment
  - Ex:

### In /etc/mail/freebsd.mc

```
VERSIONID(`$FreeBSD: src/etc/sendmail/freebsd.mc,v 1.30.2.2 2006/08/23 03:31:00 gshapiro Exp $')
```

### In /etc/mail/sendmail.cf

```
##### $Id: cfhead.m4,v 8.116 2004/01/28 22:02:22 ca Exp $ #####  
##### $Id: cf.m4,v 8.32 1999/02/07 07:26:14 gshapiro Exp $ #####  
##### $FreeBSD: src/etc/sendmail/freebsd.mc,v 1.30.2.2 2006/08/23 03:31:00 gshapiro Exp $ #####  
##### $Id: freebsd6.m4,v 1.1 2005/06/14 02:16:35 gshapiro Exp $ #####  
##### $Id: generic.m4,v 8.15 1999/04/04 00:51:09 ca Exp $ #####  
##### $Id: redirect.m4,v 8.15 1999/08/06 01:47:36 gshapiro Exp $ #####  
##### $Id: use_cw_file.m4,v 8.11 2001/08/26 20:58:57 gshapiro Exp $ #####  
##### $Id: access_db.m4,v 8.26 2004/06/24 18:10:02 ca Exp $ #####  
##### $Id: blacklist_recipients.m4,v 8.13 1999/04/02 02:25:13 gshapiro Exp $ #####  
##### $Id: local_lmtp.m4,v 8.17 2002/11/17 04:41:04 ca Exp $ #####  
##### $Id: mailertable.m4,v 8.25 2002/06/27 23:23:57 gshapiro Exp $ #####  
##### $Id: virtusertable.m4,v 8.23 2002/06/27 23:23:57 gshapiro Exp $ #####
```

# Macros

## – OSTYPE macro (1)

- Define OS type of site
  - Each OS type will correspond to one ostype.mc file
  - ostype.mc file packages a variety of vendor-specific information, including
    - Expected locations of mail-related files
    - Path to sendmail related commands
    - Flags to mailer programs
  - An ostype file looks nearly empty since everything is default

In `cf/ostype/freebsd6.mc`

```
VERSIONID(`$Id: freebsd6.m4,v 1.1 2005/06/14 02:16:35 gshapiro Exp $')
ifdef(`STATUS_FILE',, `define(`STATUS_FILE', `/var/log/sendmail.st'))dnl
dnl turn on S flag for local mailer
MODIFY_MAILER_FLAGS(`LOCAL', `+S')dnl
ifdef(`LOCAL_MAILER_PATH',, `define(`LOCAL_MAILER_PATH', /usr/libexec/mail.local))dnl
ifdef(`LOCAL_MAILER_ARGS',, `define(`LOCAL_MAILER_ARGS', `mail $u'))dnl
ifdef(`UUCP_MAILER_PATH',, `define(`UUCP_MAILER_PATH', `/usr/local/bin/uux'))dnl
ifdef(`UUCP_MAILER_ARGS',, `define(`UUCP_MAILER_ARGS', `uux - -r -z -a$g $h!rmail ($u)'))dnl
```

# Macros

## – OSTYPE macro (2)

- Part of Variable sets in ostype files
  - See cf/READE file, OSTYPE section

Variable	Default Value	Description
ALIAS_FILE	/etc/mail/aliases	Text version alias file
HELP_FILE	/etc/mail/helpfile	Information for HELP command
QUEUE_DIR	/var/spool/mqueue	Mail queue directory
STATUS_FILE	/etc/mail/statistics	Information of status
LOCAL_MAILER_PATH	/bin/mail	Program used to deliver local mail
LOCAL_MAILER_MAX	Undefined	Maximum size of local mail
LOCAL_SHELL_PATH	/bin/sh	Shell used to deliver piped email
SMTP_MAILER_MAX	Undefined	Maximum size of smtp like mailer
PROCMail_MAILER_PATH	/usr/local/bin/procmail	Path for procmail program
PROCMail_MAILER_MAX	Undefined	Maximum size of accepted by procmail

# Macros

## – OSTYPE macro (3)

- Override the default value in ostype .mc file
  - Specify them in your config.mc file
  - For example:
    - Let sendmail use multiple alias files

```
define(`ALIAS_FILE', `/etc/mail/aliases,nis:mail.aliases@+cs.nis')dnl
```

# Macros

## – DOMAIN macro

- Define DOMAIN of site
  - Each DOMAIN type will correspond to one domain.mc file
  - domain.mc file packages information common to the entire domain as you wish, usually including
    - Relay
      - Rule that sends all of one type of mail to a specific destination
      - Ex: `define(`LOCAL_RELAY',`smtp:relay.cs.nctu.edu.tw')`
    - Masquerading
      - Transforming local hostname in address into another domain name
      - Ex: `MASQUERADE_AS(cs.nctu.edu.tw)dnl`

# Macros

## – MAILER macro (1)

- Declare delivery agent you want to enable
  - Put your MAILER in the bottom of .mc file
  - MAILER(`local')
    - Always include this except if you relay all your mail to another site
      - local DA, deliver mail to user's mailbox
      - prog DA, send mail through program for delivery
  - MAILER(`smtp')
    - Support for sending email to other hosts
      - smtp DA, speak regular SMTP
      - esmtp DA, speak extended SMTP
      - smtp8 DA, send mail to server not knowing 8-bit MIME
      - dsmtpl DA, send mail on demand
      - relay DA, for transmission to various relay host

# Macros

## – MAILER macro (2)

### ○ Other MAILER

- See *sendmail/cf/READE* file, MAILER section
- usenet
  - Used to post message to USENET newsgroups
- uucp
  - Used to forward email over UUCP network
- procmail
  - procmail can be used as local delivery agent to do filtering or route mail to files
- pop
  - Provide a way to perform local delivery for user that does not have a local UNIX account
- fax
  - Used to deliver mail to a fax-sending program
  - Ex: To: joe@5554321.fax
- error
  - Used to send bounce mail with error message
- junk



# Macros

## – Masquerading related macros(1)

### ○ Masquerading

- The process of transforming local hostname in address to another domain
- Macros can be used to rewrite header-sender, header-recipient or envelope address

### ○ Related macros

- MASQUERADE\_AS(`server')
- EXPOSED\_USER(`user')
- EXPOSED\_USER\_FILE(`file')
- MASQUERADE\_DOMAIN(`otherhost.domain')
- MASQUERADE\_DOMAIN\_FILE(`file')
- MASQUERADE\_EXCEPTION(`host.domain')
- MASQUERADE\_EXCEPTION(`file')

# Macros

## – Masquerading related macros(2)

- MASQUERADE\_AS(`server')
  - Used to make all clients' mail to appear as if it is **from** the specified server
  - “From:” will be changed to masqueraded server, but “Received:” and “Message-ID:” are the same
  - Ex:
    - lwhsu@lwbsd.cs.nctu.edu.tw → lwhsu@lwhsu.cs.nctu.edu.tw
    - MASQUERADE\_AS(`cs.nctu.edu.tw')
- For Exceptions
  - EXPOSED\_USER(`user')
  - EXPOSED\_USER\_FILE(`/etc/mail/exposedusers')

```
From lwhsu@lwbsd.cs.nctu.edu.tw Wed Apr 25 13:53:36 2007
Received: from lwbsd.cs.nctu.edu.tw (lwbsd.cs.nctu.edu.tw [140.113.17.212])
    by nabsd.cs.nctu.edu.tw (Postfix) with ESMTP id 8CDE23B4E27
    for <lwhsu@nabsd.cs.nctu.edu.tw>; Wed, 25 Apr 2007 13:53:36 +0800 (CST)
Date: Wed, 25 Apr 2007 13:50:46 +0800 (CST)
From: Li-Wen Hsu <lwhsu@cs.nctu.edu.tw>
Message-Id: <200704250550.13P5okPQ044935@lwbsd.cs.nctu.edu.tw>
To: lwhsu@nabsd.cs.nctu.edu.tw
Subject: test from lwbsd
```

# Macros

## – Masquerading related macros(3)

- MASQUERADE\_AS(`server`) plus
- FEATURE(`allmasquerade`)
  - MASQUERADE\_AS will change “From:” header
  - allmasquerade feature will change “To:” header either
  - Ex:
    - MASQUERADE\_AS(`cs.nctu.edu.tw`)
    - FEATURE(`allmasquerade`)
    - lwhsu@lwbsd.cs.nctu.edu.tw → lwhsu@lwbsd.cs.nctu.edu.tw

```
From lwhsu@lwbsd.cs.nctu.edu.tw Wed Apr 25 13:54:40 2007
...
Date: Wed, 25 Apr 2007 13:54:39 +0800 (CST)
From: Li-Wen Hsu <lwhsu@cs.nctu.edu.tw>
Message-Id: <200704250554.l3P5sdpi044993@lwbsd.cs.nctu.edu.tw>
To: lwhsu@cs.nctu.edu.tw
...
```

# Macros

## – Masquerading related macros(4)

- MASQUERADE\_AS(`server')
- FEATURE(masquerade\_envelope)
  - This feature will change envelope address
  - Ex:
    - MASQUERADE\_AS(`cs.nctu.edu.tw')
    - FEATURE(`masquerade\_envelope')
    - lwhsu@lwbsd.cs.nctu.edu.tw → lwhsu@nabsd.cs.nctu.edu.tw

```
From lwhsu@cs.nctu.edu.tw Wed Apr 25 14:01:45 2007
```

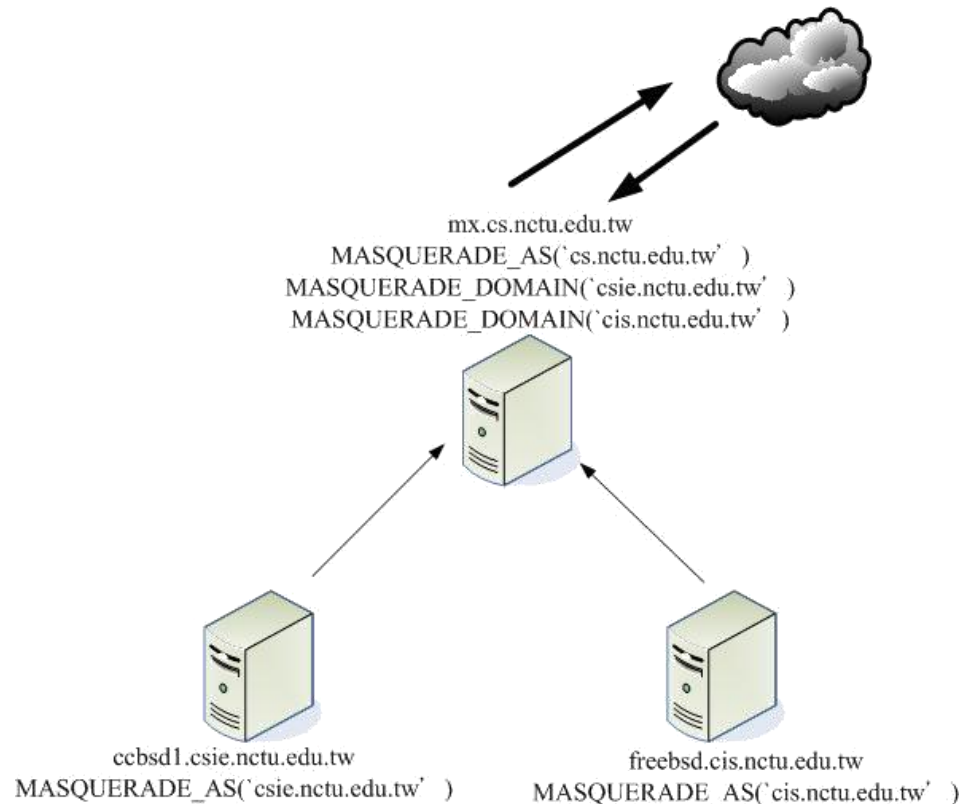
```
...  
Received: from lwbsd.cs.nctu.edu.tw (lwbsd.cs.nctu.edu.tw [140.113.17.212])  
by nabsd.cs.nctu.edu.tw (Postfix) with ESMTP id 4F0183B4E27  
for <lwhsu@nabsd.cs.nctu.edu.tw>; Wed, 25 Apr 2007 14:01:45 +0800 (CST)
```

```
...  
From: Li-Wen Hsu <lwhsu@cs.nctu.edu.tw>  
Message-Id: <200704250557.13P5vhW1045075@lwbsd.cs.nctu.edu.tw>  
To: lwhsu@nabsd.cs.nctu.edu.tw
```

# Macros

## – Masquerading related macros(5)

- MASQUERADE\_DOMAIN(`other.domain')
- MASQUERADE\_DOMAIN\_FILE(`file')
- Masquerade a domain other than your local one to the host specified in MASQUERADE\_AS
- Ex:



# Macros

## – Masquerading related macros(6)

- MASQUERADE\_EXCEPTION(`domain')
- MASQUERADE\_EXCEPTION\_FILE(`file')
- Ex:
  - MASQUERADE\_AS(`nctu.edu.tw')
  - FEATURE(`masquerade\_entire\_domain')
  - MASQUERADE\_EXCEPTION(`cs.nctu.edu.tw')

# Macros

## – FEATURE macros (1)

### ○ FEATURE

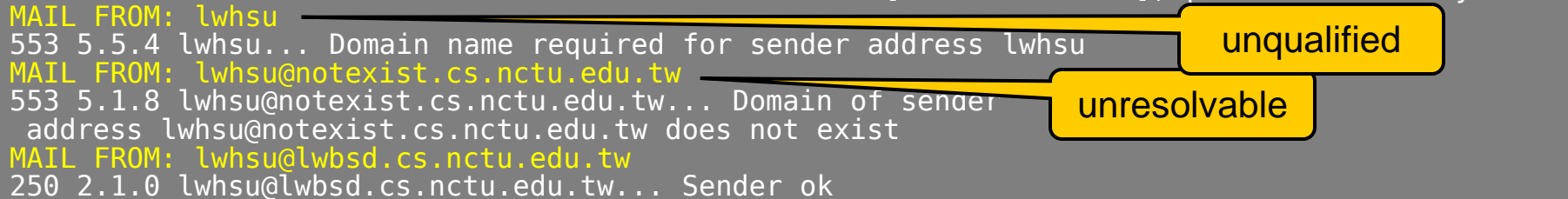
- Some useful functionality
- Macro syntax:
  - FEATURE(keyword)
  - FEATURE(keyword, argument)
  - FEATURE(keyword, argument, argument, ...)
- Each FEATURE macro declaration will cause a file in feature/keyword.mc to be used to generate .cf file
- See cf/feature directory for feature listing

# Macros

## - FEATURE macros (2)

- FEATURE(accept\_unqualified\_senders)
- FEATURE(accept\_unresolvable\_domains)

```
nabsd [/home/lwsu] -lwsu- telnet lwbsd.cs.nctu.edu.tw 25
Trying 140.113.17.212...
Connected to lwbsd.cs.nctu.edu.tw.
Escape character is '^]'.
220 lwbsd.cs.nctu.edu.tw ESMTP Sendmail 8.13.8/8.13.8; Wed, 25 Apr 2007 14:12:52 +0800 (CST)
HELO nabsd
250 lwbsd.cs.nctu.edu.tw Hello nabsd.cs.nctu.edu.tw [140.113.17.215], pleased to meet you
MAIL FROM: lwsu
53 5.5.4 lwsu... Domain name required for sender address lwsu
MAIL FROM: lwsu@notexist.cs.nctu.edu.tw
53 5.1.8 lwsu@notexist.cs.nctu.edu.tw... Domain of sender
address lwsu@notexist.cs.nctu.edu.tw does not exist
MAIL FROM: lwsu@lwbsd.cs.nctu.edu.tw
250 2.1.0 lwsu@lwbsd.cs.nctu.edu.tw... Sender ok
```





# Macros

## – FEATURE macros (3)

- FEATURE(`genericstable')
  - /etc/mail/genericstable syntax  
*user@original.domain*                      *another-user@another.domain*
  - Aliasing for outgoing mail (change From: address)
  - Rewrite only header, not envelope
    - Mail delivery is not affected, only replies
  - Only host in generic class would be looked up in table
  - To use this feature:
    - GENERICS\_DOMAIN\_FILE(`/etc/mail/local-host-names')
    - Or GENERIC\_DOMAIN(`host') macro
    - FEATURE(`genericstable')
  - Ex:
    - lwhsu                                      chonsi@gmail.com
    - lwhsu@lwbsd.cs.nctu.edu.tw → lwhsu@nabsd.cs.nctu.edu.tw

```
From lwhsu@lwbsd.cs.nctu.edu.tw Wed Apr 25 14:39:01 2007
..
From: Li-Wen Hsu <chonsi@gmail.com>
Message-Id: <200704250636.l3P6aBsM045979@lwbsd.cs.nctu.edu.tw>
To: lwhsu@nabsd.cs.nctu.edu.tw
```

# Macros

## – FEATURE macros (4)

- FEATURE(`virtusertable')
  - /etc/mail/virtusertable syntax  
*user@virtual.domain      another-user@another.domain*
  - Aliasing for incoming mail (compared with genericstable)
    - Route mail to another address (header, envelope won't be changed)
  - When local delivery, if matching entry in table, this mail will send to the specify address
  - To use this feature:
    - VIRTUSER\_DOMAIN(`vdomain')
    - Or VIRTUSER\_DOMAIN\_FILE macro
    - FEATURE(`virtusertable')
  - Ex:
    - @abc.com                      %1@real.com
    - @def.com                      haha@real.com
    - joe@gh.com                    error:No such user
  - Ex:
    - lwhsu@lwbsd.cs.nctu.edu.tw                      freg@nabsd.cs.nctu.edu.tw
    - lwhsu@lwbsd.cs.nctu.edu.tw → lwhsu@lwbsd.cs.nctu.edu.tw
      - When mail reach lwbsd.cs.nctu.edu.tw, this mail will route to nabsd.cs.nctu.edu.tw for freg. (Note: freg got one mail "To: lwhsu@lwbsd.cs.nctu.edu.tw")

# Macros

## – FEATURE macros (5)

### ○ FEATURE(`maillertable')

- /etc/mail/maillertable syntax

*old\_domain*      *mailer:user@new\_domain*

- This feature redirect mail addressed to “old\_domain” to alternate “destination” via particular “mailer” when the mail goes out from a site

### • Ex:

- ieee.org                      smtp:mgate1.csie.nctu.edu.tw
- .hinet.net                    smtp:mgate1.csie.nctu.edu.tw
- bad.csie.nctu.edu.tw              error:5.7.0:500 mail to bad is prohibited
- cg8848.com                  junk:

# Macros

## – FEATURE macros (6)

### ○ FEATURE(redirect)

- Allow aliases bounce with an indication of the new forwarding address
- This feature might cause double bounce with spam mail
- Ex: abcd@lwbsd.cs.nctu.edu.tw has moved to lwhsu@nabsd.cs.nctu.edu.tw
  - In /etc/mail/aliases

abcd: lwhsu@nabsd.cs.nctu.edu.tw.REDIRECT

```
----- The following addresses had permanent fatal errors -----  
lwhsu@nabsd.cs.nctu.edu.tw.REDIRECT  
  (expanded from: <abcd@lwbsd.cs.nctu.edu.tw>)  
  
----- Transcript of session follows -----  
551 5.1.1 User has moved; please try <lwhsu@nabsd.cs.nctu.edu.tw>
```

# Macros

## – FEATURE macros (7)

### ○ FEATURE(use\_cw\_file)

- cw\_file is the file that contains the names of all local host for which this host accepts to local delivery
- Default cw\_file is /etc/mail/local-host-names
  - Use the following macro to change this default:
  - define(`confCW\_FILE', `-o /etc/mail/local.list')
- Each client machine should contain
  - Its hostname
  - Nickname
  - Localhost
- A mail hub should contain
  - Any local hosts
  - Any accepted virtual domains

```
lwbsd  
localhost  
localhost.cs.nctu.edu.tw  
lwbsd.cs.nctu.edu.tw  
lwbsd.dyndns.org
```

```
localhost  
localhost.cs.nctu.edu.tw  
csmailgate  
csmailgate.cs.nctu.edu.tw  
csie.nctu.edu.tw  
eecsep.nctu.edu.tw
```

# Macros

## – FEATURE macros (8)

- Default
  - Local delivery agent is /bin/mail and
  - Local delivery agent use /bin/sh to pipe mail to program
- sendmail's security ones
  - mail.local and smrsh
- FEATURE(`local\_lmtp', `/usr/libexec/mail.local')
- FEATURE(`smrsh', `/usr/libexec/smrsh')
- Change shell to smrsh, the restricted shell provided by sendmail



## **Relay related macros**

Rule that sends all of one type of mail to a specific destination

# Relay Macros

## – LOCAL\_RELAY and LOCAL\_USER

- Local delivery
  - Any email address that is username only will be delivered using “local” DA
- LOCAL\_RELAY macro
  - Relay this kind of mails to other mail server
  - `define(`LOCAL_RELAY', `relay_host')`
  - Ex:
    - `define(`LOCAL_RELAY', `fastmx.cs.nctu.edu.tw')`
- LOCAL\_USER and LOCAL\_USER\_FILE macro
  - Local delivery such users even if LOCAL\_RELAY is using
  - Ex:
    - `LOCAL_USER(`operator')`



# Relay Macros

## – MAIL\_HUB

### ○ MAIL\_HUB

- Route all incoming mail to a central server for delivery
- Often used when there is a central mail box server
- Ex:
  - `define(`MAIL_HUB', `smtp:csmailgate.cs.nctu.edu.tw')`
  - In csmailgate, it use `/etc/mail/local-host-names` to decides wither to do local delivery or `/etc/mail/mailertable`, `/etc/mail/virtusertable` for further relay

# Relay Macros

## – SMART\_HOST

- SMART\_HOST
  - Make external mail relay to other mail server
- Comparison
  - LOCAL\_RELAY
    - Applied to unqualified names
  - MAIL\_HUB
    - Applied to names qualified with the name in /etc/mail/local-host-names
  - SMART\_HOST
    - Applied to name qualified with other hosts



# **Configuration Options**



# Options

## – queued mail related

- `confTO_QUEUERETURN`
  - How long a message will remain in queue if it cannot be delivered
- `confTO_QUEUEWARN`
  - How long it will sit before the sender is notified that there might be problems with delivery
- Ex:
  - `define(`confTO_QUEUERETURN', `3d')`
  - `define(`confTO_QUEUEWARN', `4h')`

# Options

## – privacy related

### ○ confPRIVACY\_FLAGS

- Used to force other sites to adhere some SMTP conventions

#### • Flags

- noetrn Disallow all SMTP ETRN commands
- noexpn Disallow all SMTP EXPN commands
- noverb Disallow all SMTP VERB commands
- novrfy Disallow all SMTP VRFY commands
- needexpnhelo Require HELO before EXPN
- needmailhelo Require HELO before MAIL FROM:
- needvrfyhelo Require HELO before VRFY
- ...

#### • Ex.

- `define(`confPRIVACY_FLAGS',  
`authwarnings,noexpn,novrfy')`

# Options

## – performance related (1)

### ○ confHOSTStatusDirectory

- When mail queue is run, sendmail will fork a child process to process each queued mail.
- Keep a file for each host's status information, which is failed to send mail
- These information can be used to prioritize the hosts when queue is run again
- Ex:
  - `define(`confHOST_STATUS_DIRECTORY', `/var/spool')`

# Options

## – performance related (2)

### ○ confFALLBACK\_MX

- Forward all undeliverable mail to a local server
- This can free the regular mail server to deliver the mail with good address

### • Ex:

- `define(`confFALLBACK_MX', `clearnerMX.cs.nctu.edu.tw')`

# Options

## – performance related (3)

### ○ confQUEUE\_LA

- Let sendmail to queue message instead of delivering it when the load comes to setting value
- Default is 8#CPU
  - `define(`confQUEUE_LA', 10)`

### ○ confREFUSE\_LA

- Let sendmail to refuse connection rather than accepting them when the load comes to setting value
- Default is 12#CPU
  - `define(`confREFUSE_LA', 15)`





# **Spam handling in sendmail**



# Strategy

- Spam handling strategy
  - Relay with care
  - Access database
  - Check against blacklist
  - Header checking

# access database (1)

## ○ Access database

- Sendmail use access database to check incoming mail to reject some specific user or domain
- Sendmail also use access database to determine whether relay host or domain
- To use access database:  
FEATURE(`access\_db', `hash -T<TMPF> /etc/mail/access')

Prepare your access in text file

```
/usr/sbin/makemap hash access.db < access  
(or just type "make maps" in /etc/mail)
```

## access database (2)

- The access file

Syntax:    LHS                      RHS

- LHS: Part of the address or user

- host.your.domain            ← a hostname
- your.domain                ← a domain name
- user@                        ← a username
- user@host.domain         ← an user address
- 123.45.67.89               ← IPv4 host address
- 123.45                      ← IPv4 network (leftmost numbers)

- With Prefix

- From: address, To:Address

- From → envelop sender, To → envelop recipient
- Address could be either the IP or hostname, with/without user@
- Ex. From:spammer@some.domain, From:cyberspammer.com

- Connect: address

- The address is ether the IP or hostname of a connecting host

# access database (3)

- RHS: action
  - OK
  - RELAY
    - Accept this mail and relay to its destination
  - REJECT
    - Reject the mail with a generic error message
    - This message can be defined in confREJECT\_MSG macro
  - DISCARD
    - Silently discard the message
  - xxx message
    - Return an error, xxx must be an RFC821 code
  - ERROR: xxx message
  - ERROR: x.x.x message
    - Return an error, x.x.x must be an RFC1893 code

# access database (4)

- Example

okay.cyberspammer.com	OK
nctu.edu.tw	RELAY
140.113	RELAY
127.0.0.1	RELAY
Galaxy.os.NCTU.edu.tw	REJECT
www@csie.nctu.edu.tw	DISCARD
#bsduser@some.domain recipient	550 Mailbox disabled for this recipient
mailman@es1.seed.net.tw recipient	550 Mailbox disabled for this recipient
mailman@postman1.seed.net.tw this recipient	550 Mailbox disabled for this recipient
61.30.99.136	REJECT
61.56.251.5	REJECT
61.70.162.11	REJECT
61.70.163.206	REJECT
...	

# Blacklisting user or sites (1)

## ○ Black user

- Use FEATURE(`blacklist\_recipients') with access table to block local users or hosts
- Ex:
  - FEATURE(`blacklist\_recipients')
  - IN /etc/mail/access
    - lwhsu@cs.nctu.edu.tw 550 Mailbox disabled for this user

## ○ DNSBL

- Block other hosts
- Domain Name Services BlackList
- It is a list of:
  - Mail server hostname that run open relays
  - Host that might be owned by known spammers

# Blacklisting user or sites (2)

- How DNSBL work
  - Normal mail transaction
    - Connect → DNS for IP → SMTP
  - DNSBL involved
    - Connect → DNS for IP → DNSBL that IP → SMTP
  - When do DNSBL
    - reverse IP
    - Append black-list related domain name
    - Lookup that hostname with DNSBL DNS server
    - If found, this IP is in the black list maintained by that org
  - Ex:
    - 123.45.67.89 is the IP
    - 89.67.45.123 is the reversed IP
    - 89.67.45.123.relay.mail-abuse.org



# Blacklisting user or sites (3)

- Some DNSBL maintainer
  - <http://www.spamcop.net/> SCBL-SpamCop Blocking List
  - <http://mail-abuse.org> Mail Abuse Prevention Systems
- Usage
  - FEATURE(`dnsbl', `dns-host', `message')
  - Ex:  
FEATURE(`dnsbl', `relays.mail-abuse.org', `Mail from \${client\_addr} rejected; see <http://mail-abuse.org/>)

# Other content

- You can find many material in sendmail
  - Ruleset and rule
  - Various configuration commands in sendmail.cf
    - R (Rule) command
    - S (Rule set) command
    - M (Mail DA) command
    - D (Define macro) command
    - C and F (Class macro) command
    - K (Database-map) command
    - O (Options) command
    - H (Header) command
  - Sendmail debug mode with `-d`
  - MAA, content-filtering program with sendmail