

Postfix / Dovecot / MySQL / PostfixAdmin / Squirrelmail Dual-Stack E-mail Server

FreeBSD Operating System Setup

Install FreeBSD 7.x or 8.x, amd64 version preferred (for AMD 64-bit CPUs or Intel-64 CPUs). The i386 version of FreeBSD will also work, but with lesser performance. In the following, the files listed as “must be in /usr/ports/distfiles” will be located and downloaded by the ports installation scripts, but in some cases it may not be able to find this. The exact name is specified so that if there is a problem you can download the files into /usr/ports/distfiles manually.

Configure static IPv4 and IPv6 addresses, DNS, etc. Following files use typical addresses. Adapt these to your network.

File /etc/rc.conf:

```
# -- sysinstall generated deltas -- # Sat Feb 12 04:45:39 2011
# Created: Sat Feb 12 04:45:39 2011
# Enable network daemons for user convenience.
# Please make all changes to this file, not to /etc/defaults/rc.conf.
# This file now contains just the overrides from /etc/defaults/rc.conf.

# nodename
hostname="us1"

# IPv4 network config
ifconfig_age0="inet 172.20.0.21 netmask 255.255.0.0"
defaultrouter="172.20.0.1"

# IPv6 network config
ipv6_enable="YES"
ipv6_ifconfig_age0="2001:470:3d:3000::21 prefixlen 64"
ipv6_defaultrouter="fe80::21b:21ff:fe1d:c159%age0"

# misc
keymap="us.iso"
moused_enable="YES"
sshd_enable="YES"
```

File /etc/resolv.conf:

```
domain hughesnet.local
search hughesnet.local
nameserver 2001:470:3d:3000::11
nameserver 2001:470:3d:3000::12
nameserver 172.20.0.11
nameserver 172.20.0.12
```

Output of *ifconfig -a*:

```
age0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=c319b<RXCSUM,TXCSUM,VLAN_MTU,...,WOL_MAGIC,VLAN_HWTSO,LINKSTATE>
```

```

ether 00:1f:c6:be:f1:e5
inet 172.20.0.21 netmask 0xffff0000 broadcast 172.20.255.255
inet6 fe80::21f:c6ff:febe:f1e5%age0 prefixlen 64 scopeid 0x1
inet6 2001:470:3d:3000::21 prefixlen 64
nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
options=3<RXCSUM,TXCSUM>
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
nd6 options=3<PERFORMNUD,ACCEPT_RTADV>

```

Output of netstat -nr:

Routing tables

Internet:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	172.20.0.1	UGS	0	13488	age0	
127.0.0.1	link#3	UH	0	0	lo0	
172.20.0.0/16	link#1	U	1	35328	age0	
172.20.0.21	link#1	UHS	0	0	lo0	

Internet6:

Destination	Gateway	Flags	Netif
Expire			
::/96	::1	UGRS	lo0 =>
default	fe80::21b:21ff:fe1d:c159%age0	UGS	age0
::1	::1	UH	lo0
::ffff:0.0.0.0/96	::1	UGRS	lo0
2001:470:3d:3000::/64	link#1	U	age0
2001:470:3d:3000::21	link#1	UHS	lo0
fe80::/10	::1	UGRS	lo0
fe80::%age0/64	link#1	U	age0
fe80::21f:c6ff:febe:f1e5%age0	link#1	UHS	lo0
fe80::%lo0/64	link#3	U	lo0
fe80::1%lo0	link#3	UHS	lo0
ff01:1::/32	fe80::21f:c6ff:febe:f1e5%age0	U	age0
ff01:3::/32	::1	U	lo0
ff02::/16	::1	UGRS	lo0
ff02::%age0/32	fe80::21f:c6ff:febe:f1e5%age0	U	age0
ff02::%lo0/32	::1	U	lo0

MySQL 5.1 Database Server Setup

This requires the file *mysql5.1.48.tar.gz* in */usr/ports/distfiles*

1. Build and install MySQL 5.1

```
# cd /usr/ports/databases/mysql51-server
# make install clean
```

(Use all default options)

2. Edit file */etc/rc.conf* and add the following line at end:

```
mysql_enable="YES"
```

3. Start MySQL

```
# /usr/local/etc/rc.d/mysql-server start
```

4. Secure MySQL root user account, delete nameless user(s):

```
# mysql -u root mysql
mysql> UPDATE user SET Password=PASSWORD('swordfish') WHERE User='root';
mysql> DELETE FROM user WHERE User='';
mysql> FLUSH PRIVILEGES;
mysql> QUIT;
```

5. Prepare file */var/db/mysql/my.cnf*

```
# cp /usr/local/share/mysql/my-medium.cnf /var/db/mysql/my.cnf
# chmod 640 /var/db/mysql/my.cnf
```

6. Edit file */var/db/mysql/my.cnf* (changes highlighted in red bold):

```
...
[mysqld]
port                = 3306
socket              = /tmp/mysql.sock
skip-locking
key_buffer          = 16M
max_allowed_packet = 10M
table_cache         = 64
sort_buffer_size    = 512K
...
# Uncomment the following if you are using InnoDB tables
innodb_data_home_dir = /var/db/mysql/
innodb_data_file_path = ibdata1:10M:autoextend
innodb_log_group_home_dir = /var/db/mysql/
# You can set .._buffer_pool_size up to 50 - 80 %
# of RAM but beware of setting memory usage too high
innodb_buffer_pool_size = 16M
innodb_additional_mem_pool_size = 2M
# Set .._log_file_size to 25 % of buffer pool size
innodb_log_file_size = 5M
innodb_log_buffer_size = 8M
innodb_flush_log_at_trx_commit = 1
innodb_lock_wait_timeout = 50
```

...

7. Restart MySQL

```
# /usr/local/etc/rc.d/mysql-server restart
```

Dovecot POP3 / IMAP4 1.2 Mail Retrieval Server Setup

This requires the following files in `/usr/ports/distfiles`:

```
dovecot-1.2.12.tar.gz
dovecot-1.2.12.managesieve-0.11.11.diff.gz
```

1. Build dovecot from FreeBSD ports:

```
# cd /usr/ports/mail/dovecot
# make install clean

(select following options: MYSQL)
```

2. Edit file `/etc/rc.conf` and add following line at end:

```
dovecot_enable="YES"
```

3. Copy sample dovecot configuration files to `/usr/local/etc`:

```
# cd /usr/local/etc
# cp /usr/local/share/examples/dovecot/dovecot.conf .
# cp /usr/local/share/examples/dovecot/dovecot-sql.conf .
```

4. Create SSL/TLS certificate for pop3s, imaps

```
# mkdir -p /etc/ssl/dovecot
# cd /etc/ssl/dovecot
# openssl req -new -x509 -nodes -out cert.pem -keyout key.pem -days 3650
```

Typical answers to questions in creating Distinguished Name:

```
Country Name: PH
State or Province Name: Cebu
Locality Name: Cebu City
Organization Name: InfoWeapons
Organizational Unit Name: IT
Common Name: www.v6home.org
Email Address: (empty line)
```

5. Edit file `/usr/local/etc/dovecot.conf` (changes highlighted in red bold):

```
protocols = imap imaps pop3 pop3s
ssl_cert_file = /etc/ssl/dovecot/cert.pem
ssl_key_file = /etc/ssl/dovecot/key.pem
login_greeting = ISP Mail Server Ready.
mail_location = maildir:/usr/local/virtual/%d/%n
first_valid_uid = 125
last_valid_uid = 125
first_valid_gid = 125
last_valid_gid = 125
protocol imap {
    mail_plugins = quota imap_quota
}
protocol pop3 {
    mail_plugins = quota
}
```

```

protocol lda {
  postmaster_address = postmaster@v6home.org
}
auth default {
  # passdb pam {
  #   args = session=yes dovecot
  # }
  passdb sql {
    args = /usr/local/etc/dovecot-sql.conf
  }
  # userdb passwd {
  #   ...
  #   args = blocking=yes
  # }
  userdb sql {
    args = /usr/local/etc/dovecot-sql.conf
  }
  client {
    path = /var/spool/postfix/private/auth
    mode = 0660
    user = postfix
    group = postfix
  }
}
}

```

6. Edit file `/usr/local/etc/dovecot-sql.conf` (changes highlighted in red bold):

```

driver = mysql
connect = host=localhost dbname=postfix user=postfix password=swordfish
default_pass_scheme = MD5
password_query = SELECT password FROM mailbox WHERE username = '%u'
user_query = SELECT maildir, 125 AS uid, 125 AS gid, \
CONCAT('maildir:storage=', FLOOR( quota / 1024 ) ) AS quota \
FROM mailbox WHERE username = '%u' AND active = '1'

```

Postfix 2.7 SMTP MTA Server Setup

This requires the following files in `/usr/ports/distfiles`:

```
postfix/postfix-2.8.0.tar.gz
```

1. Build postfix from FreeBSD ports:

```
# cd /usr/ports/mail/postfix
# make install clean
```

```
(select following options: SASL2, TLS, MYSQL)
(in Cyrus SASL options, accept all defaults)
```

```
When it asks "Would you like me to add it [y]?", reply Y
When it asks "Would you like to activate Postfix...", reply Y
```

2. Edit file `/etc/rc.conf` and add following lines at end:

```
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"

postfix_enable="YES"
```

3. Create and edit file `/etc/periodic.conf`, add following lines:

```
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"
```

4. Create SSL certificate:

```
# mkdir -p /etc/ssl/postfix
# cd /etc/ssl/postfix
# openssl req -new -x509 -nodes -out smtpd.pem -keyout smtpd.pem -days 3650
```

Typical answers to questions in creating Distinguished Name:

```
Country Name: PH
State or Province Name: Cebu
Locality Name: Cebu City
Organization Name: InfoWeapons
Organizational Unit Name: IT
Common Name: www.v6home.org
Email Address: (empty line)
```

```
# chmod 640 /etc/ssl/postfix/smtpd.pem
# chgrp -R postfix /etc/ssl/postfix
```

5. Edit file `/usr/local/etc/postfix/main.cf` (changes in red bold, everything from the "SASL CONFIG" line down is new, and should be added at the end of the file – replace `us1.v6home.org` with your nodename, and `v6home.org` with your domain name):

```
...
soft_bounce = no
...
myhostname = us1.v6home.org
...
mydomain = v6home.org
...
mydestination = localhost.$mydomain, localhost
...
relay_domains =
proxy:mysql:/usr/local/etc/postfix/mysql_relay_domains_maps.cf
...

# SASL CONFIG
#
broken_sasl_auth_clients = yes
smtpd_sender_restrictions =
    permit_sasl_authenticated,
    permit_mynetworks
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_non_fqdn_hostname,
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
    reject_unauth_destination,
    reject_unauth_pipelining,
    reject_invalid_hostname,
    reject_rbl_client list.dsbl.org,
    reject_rbl_client bl.spamcop.net,
    reject_rbl_client sbl-xbl.spamhaus.org
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

# TLS CONFIG
#
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/postfix/smtpd.pem
smtpd_tls_cert_file = /etc/ssl/postfix/smtpd.pem
smtpd_tls_CAfile = /etc/ssl/postfix/smtpd.pem
smtpd_tls_loglevel = 0
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

# MySQL Configuration
#
virtual_alias_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
virtual_gid_maps = static:125
virtual_mailbox_base = /usr/local/virtual
```

```

virtual_mailbox_domains =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_limit = 5120000
virtual_mailbox_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 125
virtual_transport = virtual
virtual_uid_maps = static:125

# Additional for quota support
#
virtual_create_maildirsize = yes
virtual_mailbox_extended = yes
virtual_mailbox_limit_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
proxy_read_maps = $local_recipient_maps $mydestination
    $virtual_alias_maps $virtual_alias_domains $virtual_mailbox_maps
    $virtual_mailbox_domains $relay_recipient_maps $relay_domains
    $canonical_maps $sender_canonical_maps $recipient_canonical_maps
    $relocated_maps $transport_maps $mynetworks
    $virtual_mailbox_limit_maps
virtual_mailbox_limit_override = yes
virtual_maildir_limit_message = Sorry quota exceeded.
virtual_overquota_bounce = yes

```

6. Edit file `/usr/local/etc/postfix/master.cf` (changes in red bold):

```

...
smtps      inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
...

```

7. Create file `/usr/local/etc/postfix/mysql_virtual_alias_maps.cf`:

```

user = postfix
password = swordfish
hosts = localhost
dbname = postfix
query = SELECT goto FROM alias WHERE address='%s' AND active = '1'

```

8. Create file `/usr/local/etc/postfix/mysql_virtual_domains_maps.cf`:

```

user = postfix
password = swordfish
hosts = localhost
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '0' and
active = '1'

```

9. Create file `/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf`:

```
user = postfix
password = swordfish
hosts = localhost
dbname = postfix
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
```

10. Create file `/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf`:

```
user = postfix
password = swordfish
hosts = localhost
dbname = postfix
query = SELECT quota FROM mailbox WHERE username='%s'
```

11. Create file `/usr/local/etc/postfix/mysql_relay_domains_maps.cf`:

```
user = postfix
password = swordfish
hosts = localhost
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '1'
```

12. Secure above files

```
# chmod 640 /usr/local/etc/postfix/mysql_*
# chgrp postfix /usr/local/etc/postfix/mysql_*
```

13. Create transport file and update transport map database:

```
# touch /usr/local/etc/postfix/transport
# postmap /usr/local/etc/postfix/transport
```

14. Edit file `/etc/aliases` (changes in red bold):

```
root: postmaster@v6home.org
```

15. Create `aliases.db` file:

```
# /usr/bin/newaliases
```

16. Create virtual directories:

```
# mkdir /usr/local/virtual
# chown -R postfix:postfix /usr/local/virtual
# chmod -R 700 /usr/local/virtual
```

Apache 2.2 Web Server Setup

This requires the following files in `/usr/ports/distfiles`:

```
apache22/httpd-2.2.15.tar.bz2
```

1. Build postfix from FreeBSD ports:

```
# cd /usr/ports/www/apache22
# make install clean

(select following options: MYSQL)
```

2. Edit file `/usr/local/etc/apache22/httpd.conf` (changes in red bold):

```
...
ServerAdmin webmaster@v6home.org
...
ServerName us1.v6home.org:80
...
# Various default settings
Include etc/apache22/extra/httpd-default.conf

# Secure (SSL/TLS) connections
Include etc/apache22/extra/httpd-ssl.conf
...
```

3. Create SSL certificate:

```
# mkdir -p /etc/ssl/apache
# cd /etc/ssl/apache
# openssl genrsa -out server.key 1024
# openssl req -new -key server.key -out server.csr
# openssl x509 -req -days 3650 -in server.csr -signkey server.key -out
server.crt
# chmod 400 /etc/ssl/apache/*
```

Typical answers to questions in creating Distinguished Name:

```
Country Name: PH
State or Province Name: Cebu
Locality Name: Cebu City
Organization Name: InfoWeapons
Organizational Unit Name: IT
Common Name: www.v6home.org
Email Address: (empty line)
```

4. Edit file `/usr/local/etc/apache22/extra/httpd-default.conf` (changes in red bold):

```
...
ServerTokens Prod
...
ServerSignature Off
...
HostnameLookups Off
...
```

5. Edit file `/usr/local/etc/apache22/extra/httpd-ssl.conf` (changes in red bold):

```
...
ServerName us1.v6home.org:443
...
ServerAdmin webmaster@v6home.org
...
SSLCertificateFile "/etc/ssl/apache/server.crt"
...
SSLCertificateKeyFile "/etc/ssl/apache/server.key"
...
```

6. Edit file `/etc/rc.conf` and add following line at end:

```
apache22_enable="YES"
```

7. Start Apache

```
# /usr/local/etc/rc.d/apache22 start
```

8. Test Apache (assuming DNS domain name has been defined, else use numeric addresses):

```
Surf to http://us1.v6home.org           (should see "It Works" page)
```

```
Surf to https://us1.v6home.org         (should see "It Works" page)
```

PHP5 Web Scripting Language for Apache Setup

This requires the following files in `/usr/ports/distfiles`:

```
php-5.3.2.tar.bz2
```

1. Build PHP5.3 from FreeBSD ports:

```
# cd /usr/ports/lang/php5
# make install clean

(select following options: APACHE)
```

2. Prepare file `/usr/local/etc/php.ini`:

```
# cd /usr/local/etc
# cp php.ini-production php.ini
# chmod 644 php.ini
```

3. Edit file `/usr/local/etc/php.ini` (changes in red bold):

```
...
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Paths and Directories ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; UNIX: "/path1:/path2"
include_path = ". "
;
; Windows: "\path1;\path2"
;include_path = ".;c:\php\includes"

...
```

4. Edit file `/usr/local/etc/apache22/httpd.conf` (changes in red bold):

```
...
<IfModule dir_module>
    DirectoryIndex index.html index.php index.php5
</IfModule>
...
...
<IfModule mime_module>
    TypesConfig etc/apache22/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddType application/x-httpd-php .php
    AddType application/x-httpd-php-source .phps
</IfModule>
```

5. Restart Apache:

```
# apachectl restart
```

6. Create test PHP script in file `/usr/local/www/apache22/data/info.php`:

```
<?php phpinfo(); ?>
```

7. Test PHP (should see multipage information including PHP variables, etc)

Surf to <http://us1.v6home.org/info.php>

Surf to <https://us1.v6home.org/info.php>

Postfixadmin Web Application Setup

This requires the following files in `/usr/ports/distfiles`:

```
postfixadmin_2.3.tar.gz
```

1. Build postfixadmin application from FreeBSD ports:

```
# cd /usr/ports/mail/postfixadmin
# make install clean
```

(accept all default options)

2. Create postfix database in MySQL. Note: the single quotes around *postfix* after “PRIVILEGES ON” are *reverse single quotes*, usually found on the same key as the tilde, or `~`. All other single quotes are the *forward single quotes*, usually found on the same key as the double quote “.

```
# mysql -u root -p
Enter password: swordfish

mysql> CREATE DATABASE postfix;
mysql> CREATE USER 'postfix'@'localhost' IDENTIFIED BY 'swordfish';
mysql> GRANT ALL PRIVILEGES ON `postfix` . * TO 'postfix'@'localhost';
mysql> FLUSH PRIVILEGES;
mysql> QUIT;
```

3. Secure postfixadmin files

```
# cd /usr/local/www/postfixadmin
# find . -type f -exec chmod 640 {} \;
# find . -type d -exec chmod 750 {} \;
```

4. Edit file `/usr/local/www/postfixadmin/config.inc.php` (changes in red bold):

```
$CONF['configured'] = true;
$CONF['postfix_admin_url'] = 'https://us1.v6home.org/postfixadmin/';
$CONF['database_type'] = 'mysql';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'postfix';
$CONF['database_password'] = 'swordfish';
$CONF['database_name'] = 'postfix';
$CONF['database_prefix'] = '';
$CONF['admin_email'] = 'postmaster@v6home.org';
$CONF['default_aliases'] = array (
    'abuse' => 'abuse@v6home.org',
    'hostmaster' => 'hostmaster@v6home.org',
    'postmaster' => 'postmaster@v6home.org',
    'webmaster' => 'webmaster@v6home.org'
);
$CONF['domain_path'] = 'YES';
$CONF['domain_in_mailbox'] = 'NO';
$CONF['aliases'] = '50';
$CONF['mailboxes'] = '50';
$CONF['maxquota'] = '1024';
$CONF['quota'] = 'YES';
$CONF['quota_multiplier'] = '1048576';
$CONF['vacation'] = 'YES';
```

```

$CONF['vacation_domain'] = 'autoreply.v6home.org';
$CONF['user_footer_link'] = 'http://us1.v6home.org/';
$CONF['footer_text'] = 'Return to v6home.org';
$CONF['welcome_text'] = <<<EOM
Hello,

Welcome to your new email account!

EOM;

$CONF['emailcheck_resolve_domain']='NO';

```

5. Create Vacation user and group accounts:

```

# pw groupadd vacation
# pw useradd vacation -c Virtual\ Vacation -d /nonexistent -g vacation -s
/sbin/nologin

```

6. Create, populate and secure vacation directory:

```

# mkdir /var/spool/vacation
# cp /usr/local/www/postfixadmin/VIRTUAL_VACATION/vacation.pl
/var/spool/vacation/
# chown -R vacation:vacation /var/spool/vacation/
# chmod 700 /var/spool/vacation/
# chmod 750 /var/spool/vacation/vacation.pl
# touch /var/log/vacation.log /var/log/vacation-debug.log
# chown vacation:vacation /var/log/vacation*

```

7. Edit file `/var/spool/vacation/vacation.pl` (changes in red bold):

```

our $db_type = 'mysql';
our $db_host = 'localhost';
our $db_user = 'postfix';
our $db_pass = 'swordfish';
our $db_name = 'postfix';
our $vacation_domain = 'autoreply.v6home.org';
our $logfile = "/var/log/vacation.log";
our $log_level = 0;
our $log_to_file = 1;
...

```

8. Edit file `/usr/local/etc/postfix/master.cf` for vacation filter (add at bottom of file):

```

vacation unix - n n - - pipe
 flags=DRhu user=vacation argv=/var/spool/vacation/vacation.pl

```

9. Edit file `/usr/local/etc/postfix/main.cf` for vacation transport (changes in red bold):

```

...
# TRANSPORT MAP
#
# See the discussion in the ADDRESS_REWRITING_README document.
transport_maps = hash:/usr/local/etc/postfix/transport
vacation_destination_recipient_limit = 1
...

```

10. Edit file `/usr/local/etc/postfix/transport` (currently empty), add following at end of file:

autoreply.v6home.org vacation:

11. Create transport map database for postfix:

```
# postmap /usr/local/etc/postfix/transport
```

12. Create new file `/usr/local/etc/apache22/Includes/postfixadmin.conf`:

```
Alias /postfixadmin/ "/usr/local/www/postfixadmin/"
<Directory "/usr/local/www/postfixadmin/">
    Options Indexes
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

13. Reload Apache configuration:

```
# apachectl configtest
# apachectl graceful
```

14. Run all startup scripts

```
# /usr/local/etc/rc.d/mysql-server start (should already be running)
# /usr/local/etc/rc.d/dovecot start
# /usr/local/etc/rc.d/postfix start
```

15. Setup postfixadmin application

Surf to <https://us1.v6home.org/postfixadmin/setup.php>

Create a password hash. Edit the generated line for `#setup_password` in file `/usr/local/www/postfixadmin/config.inc.php`.

Reload setup page. Create Super Admin account using the password just entered. The username must be an email address (not necessarily a real one). The password for the Super Admin does not need to be the same as the setup password.

16. Add a domain and user in postfixadmin

Surf to <https://us1.v6home.org/postfixadmin/>

Enter the admin username and password created during postfixadmin setup.

Click *Domain List* then *New Domain*. Enter domain name (v6home.org).

Click *Virtual List*, then *Add Mailbox*. Enter an email account (e.g. admin)

17. Test SMTP by doing telnet to the mail server on port 25

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.v6home.org.
Escape character is '^]'.
220 us1.v6home.org ESMTP Postfix
```

```
EHLO test.com
250-us1.v6home.org
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
STARTTLS
220 2.0.0 Ready to start TLS
quit
quit
```

18. Test SMTPS (SMTP over SSL) by doing telnet to the mail server on port 465

```
# telnet localhost 465
Trying 127.0.0.1...
Connected to host.domain.tld.
Escape character is '^]'.
quit
quit
```

19. Test POP3 by doing telnet to the mail server on port 110

```
# telnet localhost 110
Connected to us1.v6home.org.
Escape character is '^]'.
+OK ISP Mail Server Ready.
user admin@v6home.org (Use the account you created via the web interface)
+OK
pass xxx (Use password you just created for above user)
+OK Logged in.
list
+OK 1 messages:
1 844
.
quit
+OK Logging out
Connection closed by foreign host.
```

20. Check file `/var/log/maillog` for errors.

21. Configure an email client to connect to the mail server (e.g. Windows Live Mail).

IPv6 Support

Some minor configuration is required to make the various components support both IPv4 and IPv6.

DNS Resource Records

In a dual stack DNS server (e.g. BIND, Microsoft DNS Server, InfoWeapons SolidDNS, etc) configure both A and AAAA records for your mail server. Also configure reverse PTR records. If your DNS server is not authoritative for the reverse records, have your ISP add the necessary reverse PTR records, or have them delegate your IP address range to your public DNS server. Many mail servers will not accept mail from a sender that does not have a valid reverse DNS record. This is true for both IPv4 and IPv6. Many ISPs are not yet set up to publish reverse PTR records for IPv6. If yours is not, and you are not able to do this yourself for some reason, Hurricane Electric has a free public dual stack DNS server which you can publish your forward and reverse resource records in. See tunnelbroker.net for details.

Assuming your internal IPv4 addresses are private, you need to have both *internet* (private address) and *external* (public address) DNS servers. In BIND this can be accomplished on a single server using *views* (actually two: one *primary* and one *secondary*). In Microsoft DNS you will need two servers (actually four: an internal and external *primary* and an internal and external *secondary*).

For MX records, you should publish three priority levels. Remember that the highest priority has the lowest priority number.

High (e.g. priority 10):	AAAA record(s) of preferred mail server(s)
Middle: (e.g. priority 20):	Both AAAA and A records of preferred mail server(s)
Low: (e.g. priority 30):	A records of preferred mail server(s)

Here are typical DNS resource records in BIND 9 syntax. Of course these need to be in the appropriate forward and reverse zones. Note that `us1-v4` publishes *only* the IPv4 address, `us1-v6` publishes *only* the IPv6 address and `us1` publishes *both*. This makes it easy to set up the MX record correctly, but also allows you to force the version of IP used for a connection (e.g. to test over IPv4 from a dual stack node). There is no equivalent to the “-4” option in `ping` (to force use of IPv4) in any browsers that I know of, so this is a way to accomplish the same thing with any browser. Note that since there is no NAT (and no private addresses) in IPv6, the same addresses are used in both the internal and external views. Also note that the MX records are the same in both views, since they refer only to symbolic nodenames (not numeric IP addresses).

INTERNAL DNS RECORDS

A and AAAA records

```
; Origin added to names not ending in a dot:  
; v6home.org
```

```
us1-v4      3h    IN     A      172.20.0.21  
us1-v6      3h    IN     AAAA   2001:0470:003d:3000:0000:0000:0000:0021  
us1         3h    IN     A      172.20.0.21  
us1         3h    IN     AAAA   2001:0470:003d:3000:0000:0000:0000:0021
```

PTR/32 records

If you select the IPv6 option when you build Apache 2.2 (selected by default), the executable will include support for both IPv4 and IPv6. No special configuration is required for it to accept connections over both IPv4 and IPv6. You can check if Apache is listening for connections on either IP version with the “netstat -na” command. Unlike other servers, Apache creates a single socket that listens to both IPv4 and IPv6 (indicated by “tcp46” in netstat). Most servers create a separate socket for each IP version (indicated by “tcp4” or “tcp6”). If Apache is listening on both IP versions for non-secure HTTP (port 80) you should see a line like the following:

```
tcp46 0 0 *.80 *.* LISTEN
```

If Apache is listening on both IP versions for HTTPS (port 443) you should see a line like the following:

```
tcp46 0 0 *.443 *.* LISTEN
```

You can verify that Apache will actually *accept* connections over IPv4 and/or IPv6 in various ways:

1. Use numeric IP addresses in the browser. Remember that numeric IPv6 addresses in browser URIs must be enclosed in square brackets to keep the browser from getting confused by the colons. In a URI a colon normally indicates the following number is a nonstandard port, e.g. <http://172.20.0.1:8080>. In IPv6 you would use the URI [http://\[2001:470:3d:3000::21\]:8080](http://[2001:470:3d:3000::21]:8080) for a nonstandard port.

```
Surf to http://172.20.0.21
```

```
Surf to http://[2001:470:3d:3000::21]
```

2. Use telnet to connect to numeric IP addresses on port 80 (or optionally 443):

```
$ telnet 172.20.0.21 80
Trying 172.20.0.21...
Connected to us1.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

```
$ telnet 2001:470:3d:3000::21 80
Trying 2001:470:3d:3000::21...
Connected to us1-v6.v6home.org.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

3. Run the *info.php* script from the PHP5 installation. Connect using a nodename for the server that has both A and AAAA records defined in DNS, from a dual stack node (e.g. <http://us1.v6home.org/info.php>). In the resulting information display, check the nodename, local address and remote address entries. Since IPv6 is preferred by default when both are present, the connection should be over IPv6. You should see something like the following (under the “PHP Variables” heading) if the connection was over IPv6:

```
_SERVER["SERVER_NAME"]    us1.v6home.org
_SERVER["SERVER_ADDR"]    2001:470:3d:3000::21
_SERVER["SERVER_PORT"]    80
```

```
_SERVER["REMOTE_ADDR"] 2001:470:3d:3000::2:1
```

4. Download and install the "ShowIP" addon in the Firefox browser and then connect to your mail server (e.g. <http://us1.v6home.org/squirrelmail>). Search for "ShowIP addon". Once connected, check the IP address of the server in the lower right corner. If IPv6 is working, you should see something like "2001:470:3d:3000::21 +1". Without this addon (and anytime in Internet Explorer), there is no feedback in the browser as to whether you've connected over IPv4 or IPv6. There should be an indicator similar to the lock icon for SSL/TLS. Some *websites* will give you feedback regarding which IP you connected over, and even what address you are connecting from (the client address is available as a PHP variable as shown above). Note that there is not a PHP variable for IP version, you have to check the "remote address" for the presence of colons or periods. As an example of this, www.kame.net indicates which IP you are connecting over by having the kame "dance" when you connect over IPv6, but remain stationary when you connect over IPv4.

Postfix SMTP MTA

If you select the IPv6 option when you build postfix (selected by default), then the executable will include support for both IPv4 and IPv6, for both incoming and outgoing connections. All you need to do is to enable it in the configuration files.

There is an option which is not well documented (and not included in the distribution main.cf configuration file, even commented out). It is called "inet_protocols". It is similar to the "inet_interfaces" configuration option, but is used to enable which IP protocols are enabled. The possible values are:

inet_protocols = ipv4	IPv4 only (default)
inet_protocols = ipv6	IPv6 only
inet_protocols = ipv4,ipv6	both IPv4 and IPv6 (dual stack)
inet_protocols = all	all IP protocols (same as above)

This can be added anywhere in the main.cf file, but right after inet_interfaces would be a good place. To add IPv6 functionality to postfix (make it dual stack), add a new configuration option: "inet_protocols = all" to main.cf, and then restart postfix (or reboot server).

You can check which IP versions postfix is listening to with the "netstat -na" command. In FreeBSD, if a server is listening to port 25 over IPv4, you will see a line like the following:

```
tcp4  0      0  *.25          *.*          LISTEN
```

If a server it is listening to port 25 over IPv6, there will be a line like the following:

```
tcp6  0      0  *.25          *.*          LISTEN
```

To verify that postfix will actually *accept* incoming SMTP connections over both IPv4 and IPv6, there are two options:

1. Use numeric IP addresses in the email client for the outgoing mail server (SMTP protocol).

For IPv4, set the outgoing mail server to the numeric IPv4 address of the server (e.g. 172.20.0.21) and then try to send a message.

For IPv6, set the outgoing mail server to the numeric IPv6 address of the server (e.g. 2001:470:3d:3000::21) and then try to send a message.

2. Use telnet to connect to numeric IP addresses on port 25 (or optionally 465 for SMTPS):

```
$ telnet 172.20.0.21 25
Trying 172.20.0.21...
Connected to us1.
Escape character is '^]'.
^]
telnet> quit
Connection closed.

$ telnet 2001:470:3d:3000::21 25
Trying 2001:470:3d:3000::21...
Connected to us1-v6.v6home.org.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Verifying that postfix is actually making *outgoing* connections over IPv6 is somewhat more difficult. One way is to relay mail through it to a known dual stack email server and check the headers. These will include the numeric IP addresses of the sender and receiver on each transmission. You could also sniff an outgoing connection with Wireshark.

Dovecot POP3 and IMAP Mail Retrieval Servers

If you select the IPv6 option when you build dovecot (selected by default), then the code includes support for both IPv4 and IPv6, for both incoming connections. Neither POP3 nor IMAP makes outgoing connections (like SMTP does). All you need to do is to enable it in the configuration files.

There is an option called “listen”. By default, it is `listen=*`, which enables only IPv4. To enable IPv6, use the string `[::]`. To enable both, include both, separated by a comma. In the example configuration file, `listen=*` is included, but commented out (`#listen=*`).

<code>listen=*</code>	IPv4 only (default)
<code>listen=[::]</code>	IPv6 only
<code>listen=*,[::]</code>	both IPv4 and IPv6 (dual stack)

To add IPv6 functionality to dovecot (make it dual stack), on all enabled protocols (e.g. `pop3`, `pop3s`, `imap`, `imaps`) remove the “#” and change the “*” to “*,[::]”. Then restart dovecot (or reboot server).

You can check which IP versions the dovecot POP3 and IMAP servers are listening to with the “`netstat -na`” command.

If the POP3 server is listening over IPv4, you will see lines like the following (110 for `pop3`, 995 for `pop3s`).

```
tcp4  0      0      *.110      *.*        LISTEN
tcp4  0      0      *.995      *.*        LISTEN
```

If the IMAP server is listening over IPv4, there will be lines like the following (143 for imap, 993 for imaps):

```
tcp4  0      0      *.143      *.*        LISTEN
tcp4  0      0      *.993      *.*        LISTEN
```

If the POP3 server is listening over IPv6, you will see lines like the following (110 for pop3, 995 for pop3s).

```
tcp6  0      0      *.110      *.*        LISTEN
tcp6  0      0      *.995      *.*        LISTEN
```

If the IMAP server is listening over IPv6, there will be lines like the following (143 for imap, 993 for imaps):

```
tcp6  0      0      *.143      *.*        LISTEN
tcp6  0      0      *.993      *.*        LISTEN
```

To verify that dovecot will actually *accept* incoming pop3 and/or imap connections over both IPv4 and IPv6, there are two options:

1. Use numeric IP addresses in the email client for the outgoing mail server (SMTP protocol).

For IPv4, set the POP3 or IMAP mail server to the numeric IPv4 address of the server (e.g. 172.20.0.21) and then try to retrieve a message.

For IPv6, set the POP3 or IMAP mail server to the numeric IPv6 address of the server (e.g 2001:470:3d:3000::21) and then try to retrieve a message.

2. Use telnet to connect to the numeric IP addresses of the server on port 110 (pop3), 995 (pop3s), 143 (imap) or 993 (imaps), using both the IPv4 and IPv6 numeric addresses of the server (connections for pop3 shown below):

```
$ telnet 172.20.0.21 110
Trying 172.20.0.21...
Connected to us1.
Escape character is '^]'.
^]
telnet> quit
Connection closed.

$ telnet 2001:470:3d:3000::21 110
Trying 2001:470:3d:3000::21...
Connected to us1-v6.v6home.org.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Summary

The following output from “netstat -na” shows Apache, postfix and dovecot (among other servers) all listening for connections on both IPv4 and IPv6, nonsecure and secure. This includes port 465 (SMTP over SSL), ssh (port 22) and syslog (port 514). This is a fully dual-stack email and web server.

```

us1# netstat -na
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp6 0 0 *.995 *. * LISTEN
tcp4 0 0 *.995 *. * LISTEN
tcp6 0 0 *.110 *. * LISTEN
tcp4 0 0 *.110 *. * LISTEN
tcp6 0 0 *.993 *. * LISTEN
tcp4 0 0 *.993 *. * LISTEN
tcp6 0 0 *.143 *. * LISTEN
tcp4 0 0 *.143 *. * LISTEN
tcp6 0 0 *.465 *. * LISTEN
tcp4 0 0 *.465 *. * LISTEN
tcp6 0 0 *.25 *. * LISTEN
tcp4 0 0 *.25 *. * LISTEN
tcp4 0 0 *.3306 *. * LISTEN
tcp4 0 0 172.20.0.21.22 172.20.2.1.53822 ESTABLISHED
tcp4 0 0 *. * *. * CLOSED
tcp46 0 0 *.443 *. * LISTEN
tcp4 0 0 *. * *. * CLOSED
tcp46 0 0 *.80 *. * LISTEN
tcp6 0 0 2001:470:3d:3000.22 2001:470:3d:3000.50935 ESTABLISHED
tcp4 0 0 172.20.0.21.22 172.20.2.1.49933 ESTABLISHED
tcp4 0 0 *.22 *. * LISTEN
tcp6 0 0 *.22 *. * LISTEN
udp4 0 0 *.514 *. *
udp6 0 0 *.514 *. *

```

E-mail message header for traffic over IPv6 along the entire path

The full headers from a typical message that went IPv6 all the way follows.

The message was first sent from Outlook 2007 with an e-mail account for *lhughes@hughesnet.org*. This Outlook client ran on *lawrence-pc.hughesnet.local* (2001:470:3d:3000::2:1). The message was sent with SMTP/TLS over IPv6 to an Exchange 2007 server running on *ws1.hughesnet.org* (2001:470:3d:3000::11).

The Exchange 2007 server then retrieved the MX records from DNS (also over IPv6) for domain *v6home.org*. This directed it to deliver the message from *ws1.hughesnet.org* (2001:470:3d:3000::11) to a postfix/dovecot email server running on *us1.v6home.org* (2001:470:3d:3000::21), which hosts the email accounts for domain *v6home.org*. This transmission was also done using SMTP/TLS over IPv6.

Although it does not appear in the email headers, the message was then retrieved from the postfix/dovecot e-mail server at *us1.v6home.org* (2001:470:3d:3000::21) by the same Outlook 2007 client on *lawrence-pc.hughesnet.local* (2001:470:3d:3000::2:1), with an e-mail account for *lhughes@v6home.org*, using IMAP/SSL over IPv6.

```

Return-Path: <lhughes@hughesnet.org>
X-Original-To: lhughes@v6home.org
Delivered-To: lhughes@v6home.org

```

Received: from ws1.hughesnet.local (ws1.hughesnet.org [IPv6:2001:470:3d:3000::11])
(using TLSv1 with cipher AES128-SHA (128/128 bits))
(No client certificate requested)
by us1.v6home.org (Postfix) with ESMTPS id 660B917017
for <lhughes@v6home.org>; Sun, 13 Feb 2011 14:18:32 +0800 (PHT)

Received: from LAWRENCEPC (2001:470:3d:3000::2:1) by ws1.hughesnet.org
(2001:470:3d:3000::11) with Microsoft SMTP Server (TLS) id 8.1.436.0; Sun, 13
Feb 2011 14:22:25 +0800

From: Lawrence Hughes <lhughes@hughesnet.org>

To: <lhughes@v6home.org>

Subject: test from hughesnet.org

Date: Sun, 13 Feb 2011 14:22:23 +0800

Message-ID: <006501cbbb46\$61655050\$242ff0f0\$@org>

MIME-Version: 1.0

Content-Type: multipart/alternative;

boundary="-----_NextPart_000_0066_01CBCB89.6F889050"

X-Mailer: Microsoft Office Outlook 12.0

Thread-Index: AcvLRmA7edwNgvEqQwCP9ca+majyTA==

Content-Language: en-us