New Features in sendmail 8.10 & 8.11

Gregory Neil Shapiro
Lead Engineer
Sendmail, Inc.
<gshapiro@sendmail.org>

```
PGP 0xA00E1563: 66 39 58 9A 83 5F 52 26
                88 E4 59 36 5A 94 D9 48
```

Tutorial Overview

- Assumes a good understanding of sendmail functionality
  - Things like `$* @ $=w.$j` or `define(‘confDELIVERY_MODE’, ‘background’)` should not scare you too much
  - Eric Allman’s *Sendmail Configuration and Operation* tutorial and O’Reilly’s *sendmail* book, 2nd edition are sufficient background
- Questions and feedback encouraged
- Conventions used
  - Default paths assumed in examples
  - Use the preferred m4 style for showing configuration items
  - Include .cf syntax in parentheses if applicable

Agenda

- Groundwork
- Message Submission Agent
- SMTP Authentication
- STARTTLS
- IPv6
- Better LDAP Integration
- Policy Control
- Improved Mail Hosting
- Map Improvements
- Performance Enhancements
- Noteworthy Changes
- The Future
- Further Reading

DAEMON_OPTIONS() (O DaemonPortOptions)

- sendmail will now listen on multiple sockets
  - One for each `DAEMON_OPTIONS()` command
  - No need to run multiple sendmail daemons on one machine
- Each "daemon" socket can have different behavior, controlled by parameters
  - `DAEMON_OPTIONS(‘Name=endmail, Addr=209.220.147.187, Modifiers=bh’)`
  - New Parameters
    - `Name=`
      - Specifies a name for the daemon, used for logging (`daemon=` in `from=` syslog)
      - Available as `${daemon_name}`

`DAEMON_OPTIONS()` (`O DaemonPortOptions`)

- New parameters:
  - `Modifiers=`
    - Modifies the normal behavior according to one or more flags
    - Represented in `${daemon_flags}`
    - `a` require SMTP authentication
    - `b` bind to same interface for outgoing connection
      - Useful for virtual hosting
    - `c` perform hostname canonification
    - `f` require fully qualified hostname
    - `h` use name of interface for outgoing `HELO` command
      - Useful for virtual hosting
    - `C` do not perform hostname canonification
    - `E` disallow ETRN (see RFC 2476)
      - Required for an MSA

access DB Tags

- Provide fine grain control over lookups
- Basic tags
  - Optional, old method still works
  - `Connect:`*`{hostname,IP}`*
    - Connection information
  - `From:`*`address`*
    - Sender address or portion
  - `To:`*`address`*
    - Recipient address or portion
- Example (old and new)

```
cyberspammer.com             REJECT
sendmail.org                 RELAY

Connect:cyberspammer.com     REJECT
From:cyberspammer.com        REJECT
Connect:sendmail.org         RELAY
To:postmaster@               OK
```

Message Submission Agent (MSA)

- RFC 2476 specifies an alternate SMTP service running on port 587 (submission) for initial submission of messages
- Meant to be less strict than MTA (port 25)
  - Addresses do not have to be fully qualified
  - Hostnames do not have to be fully qualified or canonified
  - `Message-ID:` and `Date:` headers not required
- MSA makes message standards compliant before passing to an MTA

sendmail as an MSA

- Historically, sendmail acted as both MTA and MSA on port 25
- As of 8.10, by default, sendmail listens on MSA port 587 as well
  - Can be turned off using `FEATURE(‘no_default_msa’)`
  - Accomplished via new `DAEMON_OPTIONS()` (`O DaemonPortOptions`) syntax
- Future versions may make port 25 more strict
- Command line submission changing as well
  - `-G` specifies command line submission should be treated as relaying, not initial submission
  - `-U` deprecated, all non `-G` submissions considered initial submission

SMTP Authentication

- Historically, SMTP was an anonymous service
- In 8.9, promiscuous relaying turned off -- access based on host
- Not a complete solution for remote users
- SMTP Authentication provides for user authentication to the mail server
- Defined in RFC 2554, based on Simple Authentication and Security Layer (SASL) RFC 2222

Enabling SMTP Authentication

- Requires Cyrus SASL from CMU: ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/
- For security layer (optional, 8.11 only), need sfio from AT&T Research Labs: http://www.research.att.com/sw/tools/sfio/
- Compile and install Cyrus SASL and optionally sfio
- Compile sendmail with SASL and optionally sfio enabled by enabling them in `sendmail-8.11.X/devtools/Site/site.config.m4`

.../devtools/Site/site.config.m4

```
...
dnl SASL
APPENDDEF(‘conf_sendmail_ENVDEF’, ‘-DSASL’)
APPENDDEF(‘confLIBDIRS’, ‘-L/usr/local/lib’)
APPENDDEF(‘confINCDIRS’, ‘-I/usr/local/include/sasl’)
APPENDDEF(‘conf_sendmail_LIBS’, ‘-lsasl’)

dnl SFIO
APPENDDEF(‘confENVDEF’, ‘-DSFIO’)
APPENDDEF(‘confLIBS’, ‘-lsfio’)
define(‘confSTDIO_TYPE’, ‘portable’)
...
```

Note: Enabling sfio requires disabling buffered I/O
If using sfio, libsmutil and libsmdb must also be compiled with `-DSFIO`

SASL Mechanisms

- ANONYMOUS
  - No authentication required
- PLAIN
  - Like telnet, password sent as clear text
  - Uses `pwcheck_method` option in `Sendmail.conf`
- LOGIN
  - Similar to PLAIN, but proprietary (Microsoft)
- CRAM-MD5
  - APOP-style challenge response system
  - Uses shared secret, no clear text password sent
- DIGEST-MD5
  - Like CRAM-MD5 but stronger
  - Includes optional security layer support (DES or RC4)

More SASL Mechanisms

- KERBEROS_V4
  - Uses Kerberos V4 for authentication
- GSSAPI
  - Uses Kerberos V5 for authenticaion
- More to come?
  - Given that SASL is only a framework for mechanisms, new mechanisms can be plugged in
    - Secure Remote Password (SRP)
    - One Time Passwords (OTP)
    - OpenPGP

Configuring Cyrus SASL: `/usr/lib/sasl/Sendmail.conf`

- Plain text file containing lines with *option*: *value*
- `pwcheck_method`: how to check password
  - `sasldb`: Read from a private database
  - `passwd`: Read from `/etc/passwd`
  - `shadow`: Read from `/etc/shadow`
  - `PAM`: Use Pluggable Authentication Modules
  - `kerberos_v4`: Kerberos V4
  - `pwcheck`: Use supplied pwcheck daemon
- `srvtab`: where to find Kerberos V4 srvtab file
- `auth_transition`: if set to true, automatically adds secrets to sasldb when PLAIN method used

Using Cyrus SASL

- Realms
  - Grouping of users
  - PLAIN, LOGIN, and CRAM-MD5 use `user@realm` hack for secrets lookup
  - Others mechanisms have support for realms
    - Allows `user@host` to be in different realms as well
- Secrets database (sasldb)
  - Required for CRAM-MD5 and DIGEST-MD5
  - `saslpasswd [-p] [-c] [-d] [-u DOM] userid`
    - `-p`: pipe mode -- no prompt, password read on stdin
    - `-c`: create -- ask mechanisms to create the account
    - `-d`: disable -- ask mechanisms to disable the account
    - `-u` *`DOM`*: specify user domain

Configuring SMTP Authentication

- `confAUTH_MECHANISMS (O AuthMechanisms)`
  - Specifies list of mechanisms to advertise for authentication
    - Intersected with list of available mechanisms
    - Default: `GSSAPI KERBEROS_V4 DIGEST-MD5 CRAM-MD5`
- `TRUST_AUTH_MECH() ($={TrustAuthMech})`
  - Specifies list of mechanisms which are trusted to relay through the server
- `DAEMON_OPTIONS() (O DaemonPortOptions)`
  - New modifier flag `M=a` to require authentication for all connections

SMTP Authentication Configuration Continues

- `confDEF_AUTH_INFO (O DefaultAuthInfo)`
  - Path to file containing information for outbound authentication
    - Recommend: `/etc/mail/default-auth-info`
    - Contains:
      - authorization identity (userid): identifier used to check whether operations are allowed
      - authentication identity (authid): identifier used to authenticate the client
      - secret: password for authid
      - realm: authid group (optional, defaults to $j)
      - _FFR_DEFAUTHINFO_MECHS: list of mechanisms to try (optional, defaults to AuthMechanisms)
    - Example:

```
gshapiro
gshapiro
sekrit
gshapiro.net
DIGEST-MD5
```

Example SMTP Authentication Session

```
220 horsey.gshapiro.net ESMTP Sendmail 8.11.0
>>> EHLO monkeyboy.gshapiro.net
250-horsey.gshapiro.net Hello pleased to meet you
250-AUTH DIGEST-MD5 CRAM-MD5
250 HELP
>>> AUTH DIGEST-MD5
334 PDgxNDA...Lm5ldD4=
>>> QG1vbmt...OTJiODMwNGE5YjcxZTJlMzI2YjY4N2M=
250 2.0.0 OK Authenticated
>>> MAIL From:<gshapiro@gshapiro.net>
         AUTH=gshapiro@monkeyboy.gshapiro.net
250 2.1.0 <gshapiro@gshapiro.net>... Sender ok
```

SMTP Authentication and Rulesets

- New ruleset: `trust_auth`
  - Decide whether to allow client's authentication identifier to act as the requested authorization identity.
    - Do I trust Joe to authenticate for Sally?
    - If does not resolve to `$#error`, pass the same `AUTH=` information on to next hop
  - Called with the `AUTH=` parameter value of the SMTP `MAIL` command
  - Default is to only allow it if both userid and authid are the same
  - Can extend this using your own ruleset: `Local_trust_auth`

SMTP Authentication Macros

- `${auth_authen}`
  - Client's authentication credentials (authid)
- `${auth_author}`
  - The authorization identity (userid)
  - Value taken from SMTP `MAIL AUTH=` parameter
- `${auth_type}`
  - Mechanism used for authentication
- `${auth_ssf}` (8.11 only)
  - Security strength (features)
  - Set to "0" if not using security layer support or mechanism does not support security layers

Troubleshooting SMTP Authentication

- Check `Received:` header
  - `$?{auth_type}(authenticated$?{auth_ssf} (${auth_ssf} bits)$.)$.`
- Check syslog with `LogLevel` of 14 or higher
- Watch SMTP transaction (`sendmail -v`)
  - Use `-d44.4` to look for permission problems
- Check file permissions
  - `/usr/lib/sasl/*`
  - `/etc/mail/default-auth-info`
  - `/etc/sasldb`

STARTTLS (8.11 Only)

- Provides transport layer security (TLS) as specified in RFC 2478
  - TLS is a newer version of SSL
- Uses public and symmetric key cryptography and X.509 digital ceritificates
- Allows for strong encryption between MUA & MTA and between two MTAs
  - NOTE: It is ***NOT*** end to end encryption
- Can provide authentication

Enabling STARTTLS

- Require OpenSSL (http://www.openssl.org/) and sfio (http://www.research.att.com/sw/tools/sfio/)
  - Portions of OpenSSL, e.g., RSA and IDEA, are patented in the United States and various other countries and can not be used without a license
  - Commercial sendmail version from Sendmail, Inc. is based on RSA’s SSL-C
    - Legal for US residents
    - RSA does not allow us to open source the calls to their API so we can only support OpenSSL in the open source version

.../devtools/Site/site.config.m4

```
...
dnl General
APPENDDEF(‘confLIBDIRS’, ‘-L/usr/local/lib’)
APPENDDEF(‘confINCDIRS’, ‘-I/usr/local/include’)

dnl STARTTLS
APPENDDEF(‘confENVDEF’, ‘-DSTARTTLS’)
APPENDDEF(‘confLIBS’, ‘-lssl -lcrypto -lRSAglue -lrsaref’)

dnl SFIO
APPENDDEF(‘confENVDEF’, ‘-DSFIO’)
APPENDDEF(‘confLIBS’, ‘-lsfio’)
define(‘confSTDIO_TYPE’, ‘portable’)
...
```

Note: Enabling sfio requires disabling buffered I/O
libsmutil and libsmdb must also be compiled with `-DSFIO`

Digital Certificates

- Used to establish trust
- Certificate Authority
  - Trusted authority which signs other digital certificates
  - Thawte, Equifax, Verisign, etc. or roll your own
- Server Certificate
  - Certificate used for incoming connections
  - Identifies mail server to connecting client
- Client Certificate
  - Certificate used for outgoing connections
  - Identifies connecting client to mail server
  - Often the same as server certificate

OpenSSL Certificate Creation

- Create certificate authority (CA)

```
mkdir CA
cd CA
mkdir certs crl newcerts private
chmod 0700 private
echo "01" > serial
cp /dev/null index.txt
openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem
```

- Create certificate

```
umask 066
openssl req -nodes -new -x509 -keyout key.pem -out newcert.pem
```

- Sign new certificate with CA

```
openssl x509 -x509toreq -in newcert.pem -signkey key.pem -out csr.pem
openssl ca -policy policy_anything -out cert.pem -infiles csr.pem
rm -f csr.pem    # optionally remove newcert.pem (unsigned cert)
```

Configuring STARTTLS

- Setup your certificates
  - Need both the signed certificate (public) and the certificate key (private, make sure permissions are correct)
  - Keys must not be encrypted (`openssl -nodes`)
- Client/Server certificate common name (CN) should be fully qualified hostname of mail server
- Configure sendmail:

```
define(‘CERT_DIR’, ‘MAIL_SETTINGS_DIR‘’certs’)
define(‘confCACERT_PATH’, ‘CERT_DIR/’)
define(‘confCACERT’, ‘CERT_DIR/CAcert.pem’)
define(‘confSERVER_CERT’, ‘CERT_DIR/SrvCert.pem’)
define(‘confSERVER_KEY’, ‘CERT_DIR/SrvKey.pem’)
define(‘confCLIENT_CERT’, ‘CERT_DIR/CltCert.pem’)
define(‘confCLIENT_KEY’, ‘CERT_DIR/CltKey.pem’)
```

Random Settings

- TLS requires good random numbers
- sendmail uses one of the following
  - `/dev/urandom`
    - If supported by operating system, compile with `-DHASURANDOMDEV`
  - Entropy Gathering Daemon (EGD) from http://www.lothar.com/tech/crypto/
    - If `/dev/urandom` not available and EGD installed, compile with `-DEGD` and...
  - Set `confRAND_FILE (O RandFile)` option to a file containing random data or the name of the Unix socket if using EGD
    - `openssl rand -out /etc/mail/randfile -rand` *`/path/to/seed:/path/to/another:...`* `1024`
    - Regenerate frequently

STARTTLS Operation

- `STARTTLS` should appear as an ESMTP extension in `EHLO` response
  - If not, check syslog for problem reports
- `Received:` headers reflect STARTTLS usage:
  - `$?{tls_version}(using ${tls_version} with cipher ${cipher} (${cipher_bits} bits) verified ${verify})$.`
- Via rulesets, STARTTLS can be used to:
  - Allow relaying
  - Restrict incoming and/or outgoing connections
    - Require certain levels of encryption

STARTTLS Macros

- `${cert_issuer}`
  - Holds the distinguished name (DN) of the CA (certificate issuer)
- `${cert_subject}`
  - Holds the DN of the certificate owner
- `${tls_version}`
  - TLS/SSL version used for the connection
    - `TLSv1, SSLv3, SSLv2`
- `${cipher}`
  - Cipher suite used for the connection
    - E.g., `EDH-DSS-DES-CBC3-SHA`, `EDH-RSA-DES-CBC-SHA`, `DES-CBC-MD5`, `DES-CBC3-SHA`, `RC2-CBC-MD5`, `RC4-MD5`

More STARTTLS Macros

- `${cipher_bits}`
  - Keylength (in bits) of the symmetric encryption algorithm used for the connection
- `${verify}`
  - Holds the result of the verification of the presented certificate
  - Possible values:

Value	**Meaning**
OK	Verification succeeded
NO	No certificate presented
FAIL	Certificate presented but could not be verified
NONE	STARTTLS has not been performed
TEMP	Temporary error occured
PROTOCOL	Protocol error occured
SOFTWARE	Internal software error occured, connection dropped

Still More STARTTLS Macros

- `${server_name}`
  - Name of the server for the current outgoing connection
- `${server_addr}`
  - Address of the server for the current outgoing connection

Allowing Relaying with STARTTLS

- Done in ruleset RelayAuth
  - If ${verify} is OK, ${cert_issuer} is looked up in access map using CERTISSUER: tag
    - If found and RHS is RELAY, relaying is allowed
    - If found and RHS is SUBJECT, ${cert_subject} is looked up using CERTSUBJECT: tag
      - If found and RHS is RELAY, relaying is allowed
- Can also be done as a local addition to check_rcpt
  - For example, to allow relaying for *any* verifyable certificate:

```
SLocal_check_rcpt
R$*         $: $&{verify}
ROK         $#ok
```

STARTTLS Connection Restrictions in access Map

- For outbound (client) connections, lookup TLS_Srv:*hostname* or TLS_Clt:*hostname* for incoming (server) connections
- If no match, lookup TLS_Srv:*address* (or TLS_Clt)
  - In the two above tests, subdomains and subnets also tried
- If no match, lookup TLS_Srv: (or TLS_Clt:)
  - Provides a default policy
- If still no match, allow connection

STARTTLS access Map Right Hand Sides

- If previous lookup succeeds, RHS should be one of:
  - `VERIFY`
    - Certificate verification required
  - `VERIFY:`*`bits`*
    - Certificate verification required
    - `${cipher_bits}` must be at least *bits*
  - `ENCR:`*`bits`*
    - `${cipher_bits}` must be at least *bits*
- If condition satisfied, connection allowed, else rejected
  - RHS can also have `TEMP+` or `PERM+` prefix
    - Indicates temporary or permanent rejection
    - Default is temporary unless m4 `TLS_PERM_ERR` set

STARTTLS access DB Examples

```
# NOTE: CERT*: value folding for slide example only
# Allow gshapiro.net CA signed certs to relay
CERTIssuer:/C=US/ST=California/L=Emeryville/O=gshapiro.net/
            CN=Certificate+20Authority/
            Email=certificates@gshapiro.net         RELAY

# If Sendmail, Inc. CA signed cert...
CERTIssuer:/C=US/ST=California/L=Emeryville/O=Sendmail,+20Inc./
            OU=IT/CN=Sendmail+20Certification+20Officer/
            Email=rootca@sendmail.com               SUBJECT

# ... and it belongs to gshapiro@sendmail.com, allow it to relay
CERTSubject:/C=US/ST=California/L=Emeryville/O=Sendmail,+20Inc./
             OU=Engineering/CN=Gregory+20Neil+20Shapiro/
             Email=gshapiro@sendmail.com            RELAY

# Incoming 10.213.23.10: verified cert and >= 112 bit encryption
TLS_Clt:10.213.23.10                                VERIFY:112

# Outgoing 10.213.23.10: verified cert and >= 112 bit encryption
TLS_Srv:10.213.23.10                                VERIFY:112

# Outgoing smtp.sendmail.com: require >= 112 bit encryption
TLS_Srv:smtp.sendmail.com                           PERM+ENCR:112
```

IPv6

- sendmail now supports IPv6 using the API specified by RFC 2553 with some glue for systems with RFC 2133 APIs
- Currently only turned on automatically in Solaris 8
  - Others must turn on in site.config.m4 using: `APPENDDEF(‘confENVDEF’, ‘-DNETINET6’)`
  - May need other changes to conf.h
    - Linux has conf.h changes included

IPv6 Usage

- If support compiled in and available in kernel, sendmail uses IPv6
- For outgoing connections
  - Supports new AAAA DNS resource record (RR)
  - Will prefer AAAA records over A records for a hostname which has both
- For incoming connections (as daemon)
  - Can limit family via `Family=` equate in `DAEMON_OPTIONS()` (`O DaemonPortOptions`)
    - `Family=inet` for IPv4 (default)
    - `Family=inet6` for IPv6

LDAP Overhaul

- LDAP is no longer an experimental map type
  - Renamed from `ldapx` to `ldap`
- Can now search for multiple attributes
  - Use multiple attributes on the `-v` option, separated by commas
- Can now return multiple values
  - Returns first match unless `-z` option given with a separator to use
- Supports LDAP Authentication
  - `-d` *`bindDN`* specifies who to authenticate as
  - `-M` *`method`* speficies how to authenticate
    - One of `none`, `simple`, or `krbv4`
  - `-P` *`passinfo`* specifies where to find password
    - Path to a file containing the password for `simple`
    - Location of Kerberos ticket for `krbv4`

LDAP for Aliases

- Sets `-z,` automatically so multiple values are returned as comma separated string
- Use for aliases somewhat memory intensive
- Will be improved in a future version
- Example:

```
define(‘ALIAS_FILE’, ‘ldap:-k (&(objectClass=mailAlias)(uid=%0))
                         -v "uniqueMember,uniqueAlias"’)

O AliasFile=ldap:-k (&(objectClass=mailAlias)(uid=%0))
                 -v "uniqueMember,uniqueAlias"
```

LDAP Map New Flags

- `-d`, `-M`, `-P` covered already in LDAP authentication
- `-1` tells sendmail to only consider a lookup successful if exactly one match is returned
- `-r` *`deref`* specifies the LDAP alias dereference method
  - `never`: never dereference aliases (default)
  - `always`: always dereference aliases
  - `search`: only dereference aliases when searching
  - `find`: only dereference aliases when locating base object for search
- `-Z` *`size`* limits the number of values to *size*

LDAP Improvements

- New option `confLDAP_DEFAULT_SPEC` (`O LDAPDefaultSpec`) for specifying the settings to use for all future LDAP map definitions
  - Must be set before any LDAP maps defined
  - Can not be used to set `-a`, `-k`, `-N`, `-O`, `-S`, `-T`, `-v`
- Performance improvements
  - Server connection caching
    - One connection for multiple maps if host, port, and authentication matches
  - Keep connection open between lookups
  - Use asynchronous searches
    - Saves memory and network resources
- Proper RFC 2254 encoding support
  - `user=\2A` to search for `user=*`

LDAP Alias Schema for E-Mail Routing (LASER)

- `FEATURE(‘ldap_routing’)` enables LDAP-based routing of a particular address to a different host and/or a different address
- LDAP lookup is first attempted on the full address and then on the domain portion
- Applies only to domains declared as LDAP-routable via the `LDAPROUTE_DOMAIN()` m4 command
  - `LDAPROUTE_DOMAIN(‘example.com’)`

LDAP Routing Configuration

- `FEATURE(‘ldap_routing’)` has three optional arguments:
  - mailHost LDAP map definition
    - Default: `ldap -1 -v mailHost -k (&(objectClass=inetLocalMailRecipient) (mailLocalAddress=%0))`
  - mailRoutingAddress LDAP map definition
    - Default: `ldap -1 -v mailRoutingAddress -k (&(objectClass=inetLocalMailRecipient) (mailLocalAddress=%0))`
      - Note that neither of the default map definitions above includes the LDAP server hostname or base DN
      - Presumed these are set in `confLDAP_DEFAULT_SPEC` (`O LDAPDefaultSpec`) option

LDAP Routing Configuration

- Optional arguments, continued..
  - Message disposition: bounce or passthru (default)
    - If there is not a match, should the message be bounced or passed through and use the normal message routing
- Address Resolution Possibilities

mailHost is	**mailRoutingAddress is**	**Results in**
a local host	found	delivered to mailRoutingAddress
a local host	not found	delivered to original address
a remote host	found	mailRoutingAddress relayed to mailHost
a remote host	not found	original address relayed to mailHost
not defined	found	mail delivered to mailRoutingAddress
not defined	not found	deliver to original address *OR* bounced as unknown user

LDAP Routing Schema

- objectClass is `inetLocalMailRecipient`
- E-mail address listed in `mailLocalAddress` attribute
  - Can have multiple `mailLocalAddress` attributes
- If present, there must be only one `mailHost` attribute
  - Value must be a fully qualified host name
- If present, there must be only one `mailRoutingAddress` attribute
  - Value must be an RFC 822 compliant address

LDAP Routing
Schema Examples

- Deliver mail for `tom@example.com` to `thomas@mailhost.example.com`:

```
dn: uid=tom, dc=example, dc=com
objectClass: inetLocalMailRecipient
mailLocalAddress: tom@example.com
mailRoutingAddress: thomas@mailhost.example.com
```

- Relay mail for `harry@example.com` to the MX records listed for the host `mktmail.example.com` using the new address `harry@mkt.example.com`

```
dn: uid=harry, dc=example, dc=com
objectClass: inetLocalMailRecipient
mailLocalAddress: harry@example.com
mailHost: mktmail.example.com
mailRoutingAddress: harry@mkt.example.com
```

Policy Control

- New rulesets
  - Restrict SMTP `EXPN`, `VRFY`, and `ETRN` commands using `check_expn`, `check_vrfy`, and `check_etrn` rulesets
- Header checking
  - Now done on non-SMTP submissions
  - `H`*`Header`*`: $>+` *`ruleset`*
    - Do not strip comments from header value
    - `${currHeader}` contains quoted header value
    - `${hdrlen}` contains length of header
  - `H*: $>` *`ruleset`*
    - Default ruleset for header checks
    - Only called if no other ruleset already specified
    - `${hdr_name}` contains header field name
  - `check_eoh`
    - Called after end of headers

New FEATURE()’s

- `FEATURE(‘delay_checks’)`
  - `check_mail` and `check_relay` called after `check_rcpt`
  - Can give argument of `friend` or `hater`
    - Lookup `To:`*`recipient`* in access DB
    - If argument is `friend` and RHS is `SPAMFRIEND`, other rulesets skipped
    - If argument is `hater` and RHS is `SPAMHATER`, other rulesets applied
- `FEATURE(‘relay_mail_from’)`
  - Allows relaying if sender in access DB
  - If `‘domain’` argument is given, domain portion also checked

Improved Mail Hosting

- Virtual user table
  - New class for specifying virtusertable domains
    - `VIRTUSER_DOMAIN(), VIRTUSER_DOMAIN_FILE()`
    - `$={VirtHost}`
  - `FEATURE(‘virtuser_entire_domain’)` changes lookup to `$* $={VirtHost}`
  - Pass +*detail* as `%2` for lookups
- Generics table
  - `FEATURE(‘generics_entire_domain’)` changes lookup to `$* $=G`
  - Pass +*detail* as `%1` for lookups
  - Allow `@domain` entry to override masquerading

More Mail Hosting Goodies

- New `DAEMON_OPTIONS()` (`O DaemonPortOptions`) behavior
- New `confCLIENT_OPTIONS` (`O ClientPortOptions`) setting overrides outbound connection
  - Same value syntax as `DAEMON_OPTIONS()`
- New mailer flag `F=%` (`dsmtp` mailer)
  - On-demand delivery
- New macros
  - Useful for headers and rulesets
  - `${daemon_info}` (daemon info; e.g., `SMTP+queueing@00:30:00`), `${daemon_addr}`, `${daemon_family}`, `${daemon_name}`, and `${daemon_port}`
  - `${if_name}` (e.g., `ep0`) and `${if_addr}`

Maps

- `arith`
  - Math in the rulesets (`STaxes=1040`?)
    - `+`, `-`, `*`, `/`, `l` (for less than), and =
    - Coming in 8.12: `|`, &, `%`
  - `$(arith l $@ 4 $@ 2 $)` returns `FALSE`
  - `$(arith + $@ 4 $@ 2 $)` returns `6`
- `syslog`
  - Log items to syslog within ruleset
    - `K`*`name`*` syslog -L`*`priority`*
    - `R$* @ $*   $: $(`*`name`*` "User " $1 $) $1 @ $2`
- `ph`
  - Performance win for `MAILER(‘phquery’)` users

Maps, Macros, Headers Come Together

- New map, `macro`, can set or clear a macro
  - `Kmacro macro` declares the map
  - `$(macro` *`{MacName}`* `$)` clears `$`*`{MacName}`*
  - `$(macro` *`{MacName}`* `$@` *`value`* `$)` sets `$`*`{MacName}`* to *`value`*
- New class `$={persistentMacros}` saves macro values across queue runs
- New header syntax `H?`**`${`*`macro`*`}`**`?`*`Hdr`*`:` *`Val`*
- Can now set a macro in a ruleset (e.g., `check_mail`) and save that macro so when the mail is delivered, an extra header is added

Tying It All Together

```
LOCAL_CONFIG
# Maps
Kmacro macro
Karith arith

# Header checks
HTo: $>CheckTo
HCC: $>CheckTo

# Header to add
H?${BadRcpts}?X-Possible-Spam: To:/CC: ${Rcpts} recipients

# Initialize macros
D{Rcpts}0
D{MaxRcpts}20

LOCAL_RULESETS
SCheckTo
# Record the presence of the header addresses
R$* @ $*     $: $(arith + $@ $&{Rcpts} $@ 1 $) $| $2     Add 1
R$+ $| $*    $: $(macro {Rcpts} $@ $1 $) $>CheckTo $2    Save and recurse*

Scheck_eoh
# After reading headers, check ${Rcpts} > ${MaxRcpts}
R$*          $: $&{Rcpts}                                Check the macro
R$+          $: $(arith l $@ ${MaxRcpts} $@ $1 $)        Check if > max
RTRUE        $: $(macro {BadRcpts} $@ OK $)              Set macro
RFALSE       $: $(macro {BadRcpts} $)                    Clear it
R$*          $: $(macro {Rcpts} $@ 0 $)                  Reset ${Rcpts}
```

Queue Performance Improvements

- Multiple queues
  - `define(‘QUEUE_DIRECTORY’, ‘/var/q*’)`
  - `O QueueDirectory=/var/q*`
  - Directories must exist, not created
  - Can be symlinks to other partitions
  - Unsafe queues ignored
  - Daemon queue runs done in parallel
- Queue subdirectories
  - Can have one or more of `df`, `qf`, and `xf` subdirectories in each queue directory for `df`, `qf`, and `xf` files
  - Can be symlinks to other partitions (e.g., tmpfs for `xf` files)

More Queue Enhancements

- Unique queue IDs
  - Less filesystem interaction, easier moving
  - Unique only on a single host
- `confQUEUE_SORT_ORDER` (`O QueueSortOrder`)
  - New value: `filename`
    - Sorts queue in a single pass
    - Does not open each `qf` file
    - Lose benefits of other methods
  - Improved `host` method
    - Reverse hostname before sort
    - Better domain clustering

More Performance Enhancements

- Buffered file I/O
  - Only available on Torek I/O systems (BSD)
    - devtools `confSTDIO_TYPE` variable
  - Keep `df` and `xf` files in memory as long as possible (`qf` already kept in memory)
    - Until reach a certain size
      - `confXF_BUFFER_SIZE` (`O XscriptFileBufferSize`)
      - `confDF_BUFFER_SIZE` (`O DataFileBufferSize`)
    - Until require file on disk
- Only open map and alias files on demand
- Connect to servers via named sockets
  - `[IPC]` mailer with `A=FILE` *`/path/to/socket`*
  - Great for LMTP usage

Other Noteworthy Changes

- New features
  - Implement RFC 2034: Enhanced Status Codes
  - Berkeley DB 3.X support
  - Daemon control via named socket
    - `confCONTROL_SOCKET_NAME` (`O ControlSocketName`)
    - Can restart, stop, and query running daemon
  - Alternative trusted user for starting daemon, owning files
    - `confTRUSTED_USER` (`O TrustedUser`)
    - Can be used with control socket for non-root daemon control
    - Generated databases automatically changed to trusted user ownership
  - `vacation` auto-responder included

More Noteworthy Changes

- Gotchas
  - Symlink paths now checked for safety
  - `newaliases` restricted
    - Only `TrustedUser`, root, and trusted users (`$=t`)
    - `AutoRebuildAliases` deprecated
  - `PrivacyOption=goaway` no longer includes `noetrn`
  - `FEATURE('nullclient')` fully featured
  - Syntax changes for `FEATURE('nouucp')`
    - Requires argument: `reject` or `nospecial`
  - `FEATURE('rbl')` renamed `FEATURE('dnsbl')`
    - Can specify name of server and reject message:
      `FEATURE('dnsbl', 'rbl.maps.vix.com', '550 Go away')`
    - Can be included multiple times
  - Use `MAIL_SETTINGS_DIR` (defaults to `/etc/mail/`) for most configuration files
    - Filename changes: `local-host-names`, `statistics`

The Future

- 8.*soon*
  - Mail filter API (aka, Milter)
    - External message filtering on incoming SMTP
    - Filter can get connection information, `HELO/EHLO` parameter, sender, recipient(s), header(s), body
    - Filter can reject connection, recipient(s), message; discard recipient, message; add recipient(s); remove recipient(s); add header(s); replace body
  - SMTP Pipelining
- 8.*eventual* (maybe soon?)
  - Queue manager
  - Performace tuning
- 9.X
  - Separate programs
  - Threading (memory management)
  - Windows 2000© portability

For More Information

- Eric Allman's Sendmail Configuration and Operation tutorial
- O'Reilly's *sendmail* book, 2nd edition
- sendmail FAQ: http://www.sendmail.org/faq/
- Sendmail Consortium: http://www.sendmail.org/
- Sendmail, Inc: http://www.sendmail.com/ <info@sendmail.com>
- Sendmail News: http://www.sendmail.net/
- Open Source sendmail questions: <sendmail-questions@sendmail.org>