Email and Email Servers

Jack Rosenthal
2017-10-19

Mines Linux Users Group
Optional: Want to follow along?

During the second part of the presentation, you’ll have the optional opportunity to follow along in setting up your own mail server on Linux. If this means you want to spin up a cheap VPS, take a few minutes to do so.

Almost any distro will work (including FreeBSD), mine is running on Arch Linux.
Part 1: Email Concepts
What is Email?

With a friend(s)...

1. Define Email
2. Discuss what you think makes Email unique from other digital communication methods (e.g., IRC, Hangouts, Facebook, Slack, etc.)

Sorry this feels a bit like a lecture in a course... but hopefully you find this engaging.
What is Email?

- **Old:** Email is one of the oldest ways to communicate with others on a computer system (dates back to mid-60s).
- **Asynchronous:** Email replicates snail-mail’s ability to respond on what you want when you want to.
- **Protocol:** Email is a protocol, not an implementation.
- **Decentralized:** Email is dependent on no single system\(^1\).

\(^1\)although, if Gmail went down, the world may as well just give up
What is Email?

• **Old:** Email is one of the oldest ways to communicate with others on a computer system (dates back to mid-60s).

• **Asynchronous:** Email replicates snail-mail’s ability to respond on what you want when you want to.

• **Protocol:** Email is a protocol, not an implementation.

• **Decentralized:** Email is dependent on no single system\(^1\).

\(^1\)although, if Gmail went down, the world may as well just give up...
What is Email?

- **Old:** Email is one of the oldest ways to communicate with others on a computer system (dates back to mid-60s).
- **Asynchronous:** Email replicates snail-mail’s ability to respond on what you want when you want to.
- **Protocol:** Email is a protocol, not an implementation.
- **Decentralized:** Email is dependent on no single system. Although, if Gmail went down, the world may as well just give up.
What is Email?

- **Old**: Email is one of the oldest ways to communicate with others on a computer system (dates back to mid-60s).
- **Asynchronous**: Email replicates snail-mail’s ability to respond on what you want when you want to.
- **Protocol**: Email is a protocol, not an implementation.
- **Decentralized**: Email is dependent on no single system\(^1\).

\(^1\)although, if Gmail went down, the world may as well just give up
Some Definitions

**MUA**  Mail User Agent: What the user uses to send and receive Emails. Examples: Mutt, Claws Mail, Thunderbird, ...

**MTA**  Mail Transfer Agent: An agent capable of delivering Emails from one system to another. Implemented by **SMTP** (Simple Mail Transfer Protocol).

**MDA**  Mail Delivery Agent: An agent which delivers mails to a MUA. Implemented by **POP3** (Post Office Protocol 3) or **IMAP** (Internet Mail Access Protocol).
Some Definitions

**MUA** Mail User Agent: What the user uses to send and receive Emails. Examples: Mutt, Claws Mail, Thunderbird, ...

**MTA** Mail Transfer Agent: An agent capable of delivering Emails from one system to another. Implemented by **SMTP** (Simple Mail Transfer Protocol).

**MDA** Mail Delivery Agent: An agent which delivers mails to a MUA. Implemented by **POP3** (Post Office Protocol 3) or **IMAP** (Internet Mail Access Protocol).
Some Definitions

**MUA**  Mail User Agent: What the user uses to send and receive Emails. Examples: Mutt, Claws Mail, Thunderbird, ...

**MTA**  Mail Transfer Agent: An agent capable of delivering Emails from one system to another. Implemented by **SMTP** (Simple Mail Transfer Protocol).

**MDA**  Mail Delivery Agent: An agent which delivers mails to a MUA. Implemented by **POP3** (Post Office Protocol 3) or **IMAP** (Internet Mail Access Protocol).
The Path of an Email

1. Alice's MUA
   - To: bob@b.org
   - From: alice@a.org
   - Dear Bob. ...

2. DNS
   - MX for b.org?

3. mx.b.org

4. SMTP
   - mx.b.org
   - imap.b.org

5. IMAP
   - To: bob@b.org
   - From: alice@a.org
   - Dear Bob. ...

Bob's MUA

smtp.a.org
The Path of an Email

1. **Alice's MUA**
   - **To:** bob@b.org
   - **From:** alice@a.org
   - **Dear Bob. ...**

2. **mx.b.org**
   - **MX for b.org?**

3. **mx.b.org**
   - **DNS**

4. **Bob's MUA**
   - **To:** bob@b.org
   - **From:** alice@a.org
   - **Dear Bob. ...**

5. **Bob's MUA**
   - ** IMAP**

---

**smtp.a.org**

---

**mx.b.org**

---

**imap.b.org**

---

**ns.b.org**
The Path of an Email

1. Alice's MUA
   - To: bob@b.org
   - From: alice@a.org
   - Dear Bob. ...

2. MX for b.org?

3. mx.b.org

4. To: bob@b.org
   - From: alice@a.org
   - Dear Bob. ...

5. IMAP
   - Bob's MUA

smtp.a.org

mx.b.org

imap.b.org

ns.b.org
$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
Let's Send an Email (SMTP)

```
$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body

.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
```
Let's Send an Email (SMTP)

$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
Let’s Send an Email (SMTP)

$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
Let's Send an Email (SMTP)

$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
Let's Send an Email (SMTP)

```plaintext
$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
```
Let's Send an Email (SMTP)

$ telnet smtp.mines.edu 25
220 izzard.mines.edu ESMTP Sendmail 8.14.4
HELO isengard
250 izzard.mines.edu Hello isengard, pleased to meet you
MAIL From:jrosenth@mines.edu
250 2.1.0 jrosenth@mines.edu... Sender ok
RCPT To:jack@rosenth.al
250 2.1.5 jack@rosenth.al... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: This is my Email

This is the message body
.
250 2.0.0 v9J0V6dW022526 Message accepted for delivery
QUIT
221 2.0.0 izzard.mines.edu closing connection
1. Lookup MX records for `ro森th.al(po.640k.net)`

2. Connect to `po.640k.net:25`
   
   HELO izzard.mines.edu
   MAIL From:jrosenth@mines.edu
   RCPT To:jack@ro森th.al
   ...

   ...then the MTA on `po` hands the message off to the MDA, and the MUA downloads the message from the MDA.
1. Lookup MX records for `rosenth.al (po.640k.net)`

2. Connect to `po.640k.net:25`...
   
   HELO izzard.mines.edu
   MAIL From:jrosenth@mines.edu
   RCPT To:jack@rosenth.al

   ...

   ...then the MTA on `po` hands the message off to the MDA, and the MUA downloads the message from the MDA.
What did izzard do?

1. Lookup MX records for \texttt{rosenth.al(po.640k.net)}
2. Connect to \texttt{po.640k.net:25}...
   \begin{verbatim}
   HELO izzard.mines.edu
   MAIL From:jrosenth@mines.edu
   RCPT To:jack@rosenth.al
   ...
   \end{verbatim}

   ...then the MTA on \texttt{po} hands the message off to the MDA, and the MUA downloads the message from the MDA.
Part 2: Setting Up Your Own Mail Server on Linux
Postfix

- Sendmail-compatible MTA
- 1998
- Knows how to speak LMTP (Local Mail Transport Protocol)
- *Does The Job™*
Postfix

- Sendmail-compatible MTA
- 1998
- Knows how to speak LMTP (Local Mail Transport Protocol)
- *Does The Job™*
Postfix

- Sendmail-compatible MTA
- 1998
- Knows how to speak LMTP (Local Mail Transport Protocol)
- *Does The Job™*
• Sendmail-compatible MTA
• 1998
• Knows how to speak LMTP (Local Mail Transport Protocol)
• *Does The Job™*
Dovecot

- MDA, provides POP3 and IMAP
- Stores your mail
- Accepts mail by providing LMTP
- Filter mail with Pigeonhole Sieve
Dovecot

- MDA, provides POP3 and IMAP
- Stores your mail
- Accepts mail by providing LMTP
- Filter mail with Pigeonhole Sieve
Dovecot

• MDA, provides POP3 and IMAP
• Stores your mail
• Accepts mail by providing LMTP
• Filter mail with Pigeonhole Sieve
Dovecot

- MDA, provides POP3 and IMAP
- Stores your mail
- Accepts mail by providing LMTP
- Filter mail with Pigeonhole Sieve
Configuring Postfix

/etc/postfix/main.cf

myhostname = po.640k.net
mydomain = po.640k.net

# what domains to consider ourselves
mydestination = po.640k.net, localhost

# listen on all network interfaces
inet_interfaces = all

# only allow mail to us or authenticated
smtpd_relay_restrictions = permit_mynetworks,
                         permit_sasl_authenticated,
                         reject_unauth_destination
# Virtual Alias Maps

/etc/postfix/main.cf

```
# virtual domains should _not_ go
# under "mydestination"
virtual_alias_domains = rosenth.al
    steamboatnetworks.net steamboatnetworks.com
virtual_alias_maps = hash:/etc/postfix/virtual
```

/etc/postfix/virtual

```
jack@rosenth.al        jrosenth
jack@steamboatnetworks.net     jrosenth
...
```

Then run # postmap /etc/postfix/virtual
Let’s Encrypt is my drug of choice:

```
# certbot certonly --standalone -d po.640k.net

/etc/postfix/main.cf

smtpd_tls_cert_file=
    /etc/letsencrypt/live/po.640k.net/fullchain.pem
smtpd_tls_key_file=
    /etc/letsencrypt/live/po.640k.net/privkey.pem
smtpd_use_tls=yes

# Settings for POODLE and the like
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
smtp_tls_mandatory_protocols=!SSLv2,!SSLv3
smtpd_tls_protocols=!SSLv2,!SSLv3
smtp_tls_protocols=!SSLv2,!SSLv3
```
Let’s Encrypt is my drug of choice:

```bash
# certbot certonly --standalone -d po.640k.net
```

```bash
/etc/postfix/main.cf

smtpd_tls_cert_file = /etc/letsencrypt/live/po.640k.net/fullchain.pem
smtpd_tls_key_file = /etc/letsencrypt/live/po.640k.net/privkey.pem
smtpd_use_tls = yes

# Settings for POODLE and the like
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3
smtp_tls_mandatory_protocols = !SSLv2,!SSLv3
smtpd_tls_protocols = !SSLv2,!SSLv3
smtp_tls_protocols = !SSLv2,!SSLv3
```
Let's Encrypt is my drug of choice:
# certbot certonly --standalone -d po.640k.net

**/etc/postfix/main.cf**

```conf
smtpd_tls_cert_file=
  /etc/letsencrypt/live/po.640k.net/fullchain.pem
smtpd_tls_key_file=
  /etc/letsencrypt/live/po.640k.net/privkey.pem
smtpd_use_tls=yes

# Settings for POODLE and the like
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
smtp_tls_mandatory_protocols=!SSLv2,!SSLv3
smtpd_tls_protocols=!SSLv2,!SSLv3
smtp_tls_protocols=!SSLv2,!SSLv3
```
Uncomment each of the following lines:

```
/etc/postfix/master.cf

smtp    inet    n  -n  -  -  smtpd
submission    inet    n  -n  -  -  smtpd
smtps    inet    n  -n  -  -  smtpd
-o smtpd_tls_wrappermode=yes
```

If you enable `smtps` as above, Linux will not know what port to put it on. Add to `/etc/services`:

```
smtps        465/tcp
```
Uncomment each of the following lines:

```
/etc/postfix/master.cf

smtp   inet   n - n - -   smtpd
submission inet  n - n - -  smtpd
smtps   inet  n - n - -  smtpd
-o smtpd_tls_wrappermode=yes
```

If you enable `smtps` as above, Linux will not know what port to put it on. Add to `/etc/services`:

```
smtps       465/tcp
```
1. Start Postfix (change as needed for init systems):
   
   # systemctl start postfix

2. Send yourself an Email:
   
   $ fortune | mail jrosenth@mines.edu
Dovecot Setup

1. Copy sample configs from
   /usr/share/doc/dovecot/example-config
to /etc/dovecot

2. Edit /etc/dovecot/dovecot.conf:

   ```
   # Protocols we want to be serving
   protocols = imap lmtp
   ```

3. cd to /etc/dovecot/conf.d and get ready to edit a lot of files
1. Copy sample configs from 
/usr/share/doc/dovecot/example-config
to /etc/dovecot

2. Edit /etc/dovecot/dovecot.conf:

```
# Protocols we want to be serving
protocols = imap lmtp
```

3. cd to /etc/dovecot/conf.d and get ready to edit a lot of files
1. Copy sample configs from 
   /usr/share/doc/dovecot/example-config
to /etc/dovecot
2. Edit /etc/dovecot/dovecot.conf:

   # Protocols we want to be serving
   protocols = imap lmtmp

3. cd to /etc/dovecot/conf.d and get ready to edit a lot of files
Mailbox Storage Format

You’ll need to decide how you want to store mail:

**mbox**  Traditional UNIX mailbox storage format: one file per mailbox.

**maildir**  Directories with one file per message.

**sdbox**  Dovecot’s own high performance storage format (one message per file).

**mdbox**  Dovecot’s own high performance storage format (multiple messages per file).

Set your choice in `10-mail.conf`:

```
mail_location = mdbox:~/.mdbox
```
You’ll need to decide how you want to store mail:

**mbox**  Traditional UNIX mailbox storage format: one file per mailbox.

**maildir**  Directories with one file per message.

**sdbox**  Dovecot’s own high performance storage format (one message per file).

**mdbox**  Dovecot’s own high performance storage format (multiple messages per file).

Set your choice in `10-mail.conf`:

```
mail_location = mdbox:~/.mdbox
```
You’ll need to decide how you want to store mail:

**mbox**  Traditional UNIX mailbox storage format: one file per mailbox.

**maildir**  Directories with one file per message.

**sdbox**  Dovecot’s own high performance storage format (one message per file).

**mdbox**  Dovecot’s own high performance storage format (multiple messages per file).

Set your choice in **10-mail.conf**:

```
mail_location = mdbox:~/mdbox
```
Mailbox Storage Format

You’ll need to decide how you want to store mail:

- **mbox**: Traditional UNIX mailbox storage format: one file per mailbox.
- **maildir**: Directories with one file per message.
- **sdbox**: Dovecot’s own high performance storage format (one message per file).
- **mdbox**: Dovecot’s own high performance storage format (multiple messages per file).

Set your choice in `10-mail.conf`:

```
mail_location = mdbox:~/mdbox
```
You’ll need to decide how you want to store mail:

**mbox**  Traditional UNIX mailbox storage format: one file per mailbox.

**maildir**  Directories with one file per message.

**sdbox**  Dovecot’s own high performance storage format (one message per file).

**mdbox**  Dovecot’s own high performance storage format (multiple messages per file).

Set your choice in `10-mail.conf`:

```
mail_location = mdbox:~/mdbox
```
Authentication

10-auth.conf

# given user@example.com, username is "user"
auth_username_format = %Ln

Need to ask PAM to let us check:

/etc/pam.d/dovecot

auth required pam_unix.so nullok
account required pam_unix.so
# given user@example.com, username is "user"
auth_username_format = %Ln

Need to ask PAM to let us check:

/etc/pam.d/dovecot
auth    required    pam_unix.so nullok
account required    pam_unix.so
### 10-master.conf

```bash
service auth {
    unix_listener /var/spool/postfix/private/auth {
        mode = 0660
        user = postfix
        group = postfix
    }
}
```

### /etc/postfix/main.cf

```bash
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
```
Wiring-up LMTP to Postfix

10-master.conf

```conf
service lmtp {
    unix_listener /var/spool/postfix/private/lmtp {
        mode = 0660
        user = postfix
        group = postfix
    }
}
```

/etc/postfix/main.cf

```conf
mailbox_transport = lmtp:unix:private/lmtp
```
SSL/TLS in Dovecot

10-ssl.conf

ssl = required
ssl_cert =
    </etc/letsencrypt/live/po.640k.net/fullchain.pem
ssl_key =
    </etc/letsencrypt/live/po.640k.net/privkey.pem

See config files for POODLE settings and the like.
SSL/TLS in Dovecot

<table>
<thead>
<tr>
<th>10-ssl.conf</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl = required</td>
</tr>
<tr>
<td>ssl_cert =</td>
</tr>
<tr>
<td>&lt;/etc/letsencrypt/live/po.640k.net/fullchain.pem</td>
</tr>
<tr>
<td>ssl_key =</td>
</tr>
<tr>
<td>&lt;/etc/letsencrypt/live/po.640k.net/privkey.pem</td>
</tr>
</tbody>
</table>

See config files for POODLE settings and the like.
Fire up Dovecot and restart Postfix:

```
# systemctl start dovecot
# systemctl restart postfix
```

Now, send some test emails!
Fire up Dovecot and restart Postfix:

```
# systemctl start dovecot
# systemctl restart postfix
```

Now, send some test emails!
Questions?
This presentation was from the Mines Linux Users Group. A mostly-complete archive of our presentations can be found online at https://lug.mines.edu.

Individual authors may have certain copyright or licensing restrictions on their presentations. Please be certain to contact the original author to obtain permission to reuse or distribute these slides.