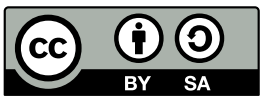
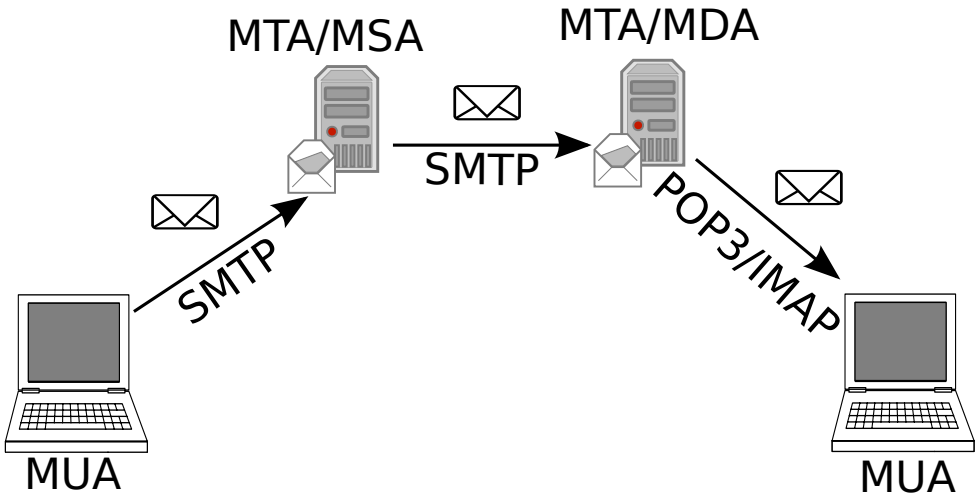
Mailserver Teil 1

Andreas Teuchert

16. Februar 2015



Übersicht



Das Bild illustriert den Weg einer E-Mail vom Sender zum Empfänger. Der Sender benutzt einen Mail User Agent (MUA), auch Mail-Client genannt um die E-Mail zu schreiben und sendet diese dann über SMTP an einen Mail Submission Agent (MSA), also seinen ausgehenden Mail-Server. Der MSA übergibt die E-Mail zur Zustellung an einen Mail Transfer Agent (MTA). Dieser sendet die E-Mail per SMTP an den Mail-Server des Empfängers, wo sie von einem Mail Delivery Agent (MDA) in dessen Postfach gespeichert wird bis er sie über POP3 oder IMAP abholt. Wie in diesem Beispiel sind MTA und MSA bzw. MTA und MDA häufig kombiniert. Dies muss aber nicht immer der Fall sein.

Die Terminologie der Mail Agents statt einfach Mail-Server und Mail-Client ist zweckmäßig, da manche Komponenten sowohl als Client als auch als Server auftreten. MTAs nehmen E-Mails als Server entgegen, übermitteln diese aber auch als Clients an andere MTAs. Ein Mail-„Server“ ist daher sowohl Client als auch Server.

Mail-Client

- auch Mail User Agent (MUA) genannt
- sendet Mail üblicherweise per SMTP an den Mail Submission Agent (MSA)
- empfängt Mail üblicherweise per POP3 oder IMAP
- muss sich gegenüber dem Mail-Server authentifizieren

Ein MUA wird vom Benutzer zum Verfassen, Versenden, Empfangen und Lesen von E-Mails verwendet. Ausgehende E-Mails werden über SMTP an den MSA gesendet, zum Empfangen wird üblicherweise POP3 oder IMAP verwendet. Auf die Diskussion proprietärer Protokolle und Schnittstellen wird an dieser Stelle verzichtet.

Heutzutage ist es üblich, dass der Client sich gegenüber dem Server sowohl zum Versenden als auch zum Empfangen authentifizieren muss. Gelegentlich reicht es zum Versenden über einen bestimmten Mail-Server auch aus, sich in dem dazugehörigen IP-Adress-Bereich zu befinden. In den Anfangszeiten des Internets war dies nicht üblich. So genannte Open Relays akzeptierten damals E-Mails von beliebigen Clients. In den 90er Jahren führte dies zu einem verstärkten Spam-Aufkommen, da Spam-Versender diese Open Relays missbrauchten. Der Betrieb von Open Relays ist daher inzwischen verpönt und wird schnell dazu führen, dass der Server auf Blacklists landet oder vom Internet-Provider gesperrt wird.

Mail-Server

- prinzipiell drei unabhängige Komponenten
- Mail Submission Agent (MSA)
  - empfängt E-Mail vom MUA und leitet sie an den MTA weiter
- Mail Transfer Agent (MTA)
  - empfängt E-Mails für lokale Adressen und sendet E-Mails für entfernte Adressen zum zuständigen MTA
- Mail Delivery Agent (MDA)
  - speichert E-Mails im lokalen Postfach
- MTA, MSA, MDA können getrennt oder kombiniert sein

Ursprünglich gab es keine Trennung zwischen MTA und MSA. Erst die Notwendigkeit der Authentifizierung von Clients führte zur Unterscheidung zwischen MTA und MSA. Während ein MTA von beliebigen[1] Clients (anderen MTAs) E-Mails annimt (aber nur für die Domains, für die er zusändig ist), nehmen MSAs nur von authentifizierten Clients E-Mails an. Dafür dürfen diese authentifizierten Clients üblicherweise E-Mails an beliebige Adressen über den MSA versenden. Um das Versenden von Spam durch authentifizierte Clients zu unterbinden, dürfen diese üblicherweise auch nur ihre eigene Adresse als Absender verwenden. Bei nicht-authentifizierten Clients ist eine solche Überprüfung im allgemeinen nicht möglich.

[1] Zur Spam-Bekämpfung nehmen die meisten MTAs keineswegs von jedem Client E-Mails an. Neben Blacklists mit bekannten Adressen von Spammern werden z. B. auch Listen mit dynamischen IP-Adressen verwendet um E-Mails von Spam-verdächtigen Clients abzulehnen.

Simple Mail Transfer Protocol (SMTP)

- Text-basiertes Protokoll zwischen MUA, MSA und MTA
- verwendet Port 25/TCP
- 465/TCP für SMTP über SSL (soll nicht mehr verwendet werden)
- heutzutage wird Extended SMTP (ESMTP) verwendet
- unterstützt Verschlüsselung (STARTTLS) und Authentifizierung
- 587/TCP für Submission (MUA zu MSA)
- aktuell in RFC 5321 definiert

MTAs, MSAs und MUAs verwenden zur Kommunikation untereinander das Simple Mail Transfer Protocol (SMTP). Üblicherweise wird dafür der TCP-Port 25 verwendet. Dieses Protokoll ist Text-basiert und war ursprünglich unverschlüsselt. Der erste Versuch SMTP verschlüsselt zu verwenden war SMTPS über Port 465. Inzwischen ist es aber üblich stattdessen ESMTP zu verwenden. Damit kann auch über Port 25 mit Hilfe von STARTTLS verschlüsselt kommuniziert werden.

Zur Kommunikation von MUA zu MSA wird inzwischen Port 587 verwendet. Es kommt zwar auch hier (E)SMTP zum Einsatz, allerdings ist dieser Port auch aus vielen Netzen erreichbar, die Port 25 zur Spam-Vermeidung filtern.

SMTP – Beispiel

```
$ telnet mailserver.example.com 25
Trying 2001:db8:f00:b1a::4711...
Connected to mailserver.example.com.
Escape character is '^]'.
220 mailserver.example.com ESMTP
HELO dude-mbp.example.com
250 mailserver.example.com
MAIL FROM:<dude@example.com>
250 2.1.0 Ok
RCPT TO:<walter@example.org>
250 2.1.5 Ok
```


Das Beispiel zeigt den ersten Teil eines SMTP-Dialogs. Nach der Verbindung zum Mail-Server auf Port 25 grüßt dieser den Client mit dem Status-Code 220 und der Nachricht `mailserver.example.com ESMTP`.

SMTP verwendet dreistellige Status-Codes, mit denen der Server dem Client signalisiert, ob der vorherige Befehl erfolgreich war. 200er und 300er Status-Codes bedeuten, dass der Befehl erfolgreich war. 400er Status-Codes bedeuten, dass ein temporärer Fehler aufgetreten ist und der Client es später erneut versuchen soll. 500er Status-Codes bedeuten, dass ein dauerhafter Fehler aufgetreten ist, ein erneuter Versuch also nicht sinnvoll ist.

Der Client identifiziert sich dann mit dem HELO-Befehl gegenüber dem Server, was wiederum mit dem Status-Code 250 quitiert wird.

Danach gibt der Client mit MAIL FROM die Absender-Adresse der E-Mail an. Der Server hat in der Regel keine Möglichkeit diese Angabe zu überprüfen.

Mit RCPT TO gibt der Client den Empfänger der E-Mail an. Ein Mail-Server wird von unauthentifizierten Clients nur E-Mails für lokale Empfänger annehmen. Andernfalls handelt es sich um ein fehlerhaft konfiguriertes Open Relay.

SMTP – Beispiel – Forts.

```
DATA
354 End data with <CR><LF>.<CR><LF>
From: Jeff Lebowski <dude@example.com>
To: Walter Sobchak <walter@example.org>
Subject: Bowling

Yo Walter -

Bowling tonite?

--Dude
.
250 2.0.0 Ok: queued as 6A8C740014
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```


Nach der Angabe von Sender- und Empfänger-Adresse signalisiert der Client mit dem DATA-Befehl, dass er nun den Inhalt der E-Mail übertragen wird. Der Server sendet daraufhin den Status-Code 354, womit der Client zum Beginn der Übertragung aufgefordert wird.

Als erstes wird der E-Mail-Header gesendet. Dieser enthält zumindest Absender, Empfänger und Subject. Üblicherweise enthält der Header noch weitere Daten, die hier zur Vereinfachung weggelassen wurden. Die hier angegebenen Absender- und Empfänger-Adressen werden dem Emfänger von seinem MUA angezeigt. Die vorher im SMTP-Dialog übermittelten Envelope-Adressen (MAIL FROM, RCPT TO) werden nur von den MTAs/MDAs zur Zustellung verwendet. Envelope- und Header-Adresen müssen auch nicht notwendigerweise übereinstimmen.

Vom Header durch eine Leerzeile abgetrennt folgt der Inhalt der E-Mail, auch Body genannt. Danach wird die E-Mail durch einen „.“, der allein in einer Zeile steht beendet.

Der Mail-Server bestätigt nun die Annahme der E-Mail mit 250 und der Client beendet den Dialog mit dem QUIT-Befehl.

ESMTP

- Client sendet EHLO statt HELO
- signalisiert damit ESMTP-Unterstützung
- Server sendet die unterstützten Erweiterungen als Antwort
- Client kann dann ESMTP-Befehle verwenden
- z. B. AUTH zur Authentifizierung und STARTTLS zur verschlüsselten Kommunikation

Das ursprüngliche SMTP sah keine Verschlüsselung und Authentifikation vor. Ebenfalls fehlten weitere, heute gewünschte, Features. Aus diesem Grund wurde das heute übliche Extended SMTP (ESMTP) eingeführt. Inzwischen wird ESMTP von allein Clients und Servern unterstützt. ESMTP verändert den SMTP-Dialog nur marginal. Im folgenden ist ein beispielhafter ESMTP-Dialog gezeigt:

```
220 mail.example.com ESMTP
EHLO client.example.com
250-mail.example.com
250-PIPELINING
250-SIZE 524288000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
QUIT
221 2.0.0 Bye
```

DNS und E-Mail

- auf der rechten Seite des @ in der E-Mail-Adresse steht die Domain, zu der die Adresse gehört
- um den zuständigen Mail-Server zu ermitteln, wird der MX-Eintrag zu der Domain über DNS abgefragt
- MX: Mail Exchanger
- existiert kein MX-Eintrag wird die Domain als Adresse des Mail-Servers behandelt und direkt der A-/AAAA-Eintrag dazu aufgelöst

MX-Eintrag abfragen

```
$ host -t MX example.org
example.org mail is handled by 10 fks1.example.org.
example.org mail is handled by 50 lax1.example.org.
```

- für example.org sind zwei Mail-Server zuständig
- 10 und 50 sind die *preference*-Werte der Mail-Server
- Server mit niedrigeren Werten werden bevorzugt
- häufig: Haupt-Mail-Server mit niedriger *preference*, Backup-Mail-Server mit höherer *preference*
- auch gleiche Werte möglich (Load-Balancing)

Postfix

- 1997 von IBM-Forscher Wietse Venema entwickelt
- sollte den damaligen Standard-Mailserver Sendmail ersetzen
- modulare Architektur
- kombiniert MTA, MSA und einen einfachen MDA
- Hauptkonfiguration unter `/etc/postfix/main.cf`
- Konfigurations-Optionen in `man 5 postconf` erklärt
- Aliases in `/etc/aliases`

Postfix-Konfiguration

- bei der Installation des Debian-Pakets `postfix` wird automatisch eine `main.cf` angelegt
- Auswahl aus fünf Konfigurations-Typen
  - No configuration
  - Internet Site
  - Internet with smarthost
  - Satellite system
  - Local only

Wird nur eine einfache Postfix-Konfiguration benötigt, kann diese bei der Installation des Postfix-Pakets unter Debian automatisch erzeugt werden. Dafür stehen vier grundlegende Konfigurations-Typen zur Auswahl.

„Internet Site“ ist für Mail-Server gedacht, die direkt E-Mails empfangen und senden. Hier wird aber üblicherweise noch weitere Konfiguration nötig sein, um einen reibungslosen Betrieb zu gewährleisten. Dies setzt aber einige Erfahrung voraus.

Bei der Konfigurations-Option „Internet with smarthost“ werden E-Mails zwar direkt empfangen, aber über ein Mail-Relay, auch smarthost genannt, versendet. Auch hier ist Vorsicht angebracht.

Ein „Satellite system“ empfängt keine E-Mails von außen. Lokale E-Mails werden entweder lokal gespeichert oder über ein Mail-Relay versandt. Dies ist eine sinnvolle Option für allgemeine Server, die gelegentlich E-Mails an den Administrator senden (z. B. Ausgaben von CRON-Jobs).

Bei „Local only“ werden keine E-Mails von außen angenommen und alle lokal erzeugten E-mails lokal gespeichert. Dies ist z. B. für Systeme ohne Möglichkeit zum E-Mail-Versand sinnvoll.

Postfix-Konfiguration – Forts.

- hier verwendete Konfiguration: Satellite system
- es werden keine E-Mails von außen angenommen
- E-Mails für lokale Benutzer werden in Mail-Boxen in `/var/mail/` gespeichert
- E-Mails an externe Adressen werden über ein Mail-Relay (Smarthost) versandt
- Weiterleitungen über `/etc/aliases`
- als Absender-Domain wird der System mail name verwendet
- Evtl. Adress-Umschreibung über Canonical-Maps

Bei der Entscheidung für die Option „Satellite system“, wird noch nach einem System mail name gefragt, welcher als Absender-Domain verwendet wird. Ebenfalls muss die Adresse des Mail-Relays angegeben werden. Diese muss in eckige Klammern gesetzt werden, damit Postfix nicht versucht, den MX-Eintrag dieser Adresse aufzulösen und die E-Mails direkt an die angegeben Adresse sendet.

Die lokal gespeicherten E-Mails können z. B. mit dem Programm `mutt` gelesen werden.

Sollen E-Mails nicht lokal gespeichert, sondern stattdessen weitergeleitet werden, können Einträge in der Datei `/etc/aliases` angelegt werden.

/etc/aliases

- in `/etc/aliases` sind Weiterleitungen definiert
- üblicherweise werden generische Adressen (z. B. postmaster und root) an einen Benutzer oder die E-Mail-Adresse des Admins weitergeleitet
- ein Eintrag pro Zeile
- Format: `adresse: ziel`
- `adresse` ist immer nur der Teil vor dem @
- `ziel` kann eine lokale Adresse ohne @ oder eine entfernte Adresse sein
- Beispiel: `root: sgroves@example.com`
- nach Änderungen `newaliases` aufrufen

Durch einen Eintrag in `/etc/aliases` werden E-Mails an die angegebene Adresse einfach an die Ziel-Adresse weitergeleitet. Die Adressen im Header werden dabei nicht umgeschrieben. Dadurch bleibt die Original-Adresse im Header erhalten.

Da Postfix statt `/etc/aliases` aus Performanz-Gründen eine Datenbank-Datei verwendet, muss diese nach dem Ändern der `/etc/aliases` mit dem Befehl `newaliases` neu erzeugt werden.

Canonical-Maps

- ermöglichen Umschreiben von Absender- und Empfänger-Adressen
- z. B. sinnvoll wenn der System mail name keine gültige Absender-Domain ist
- oder wenn keine E-Mail von/an `root@example.com` gesendet werden sollen
- in `main.cf`:
  `canonical_maps = hash:/etc/postfix/canonical`
- Format wie `/etc/aliases`
- nach Änderungen `postmap /etc/postfix/canonical` aufrufen

Durch einen Eintrag in den Canonical-Maps schreibt Postfix sowohl Absender- als auch Empfänger-Adressen um, wenn diese auf die angegebe Adresse passen. Bei geänderter Empfänger-Adresse wird die E-Mail auch dahin weitergeleitet. Im Header sind danach nur noch die umgeschriebenen Adressen zu finden.

Daher ist dies ein einfacher Weg um ungültige Adressen in lokal erzeugten E-Mails in gültige Adressen umzuschreiben.

Auch hier verwendet Postfix nicht direkt die angegebene Datei. Daher muss nach Änderungen an der Datei der `postmap`-Befehl zum Aktualisieren der Datenbank verwendet werden.

Lab 11.1: Postfix installieren

- Postfix installieren
- Aliases konfigurieren
- Test-Mail an root senden