E-Mail

by

Dr. Günter Kolousek

E-Mail

- MIME (Multipurpose Internet Mail Extensions)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol)
- IMAP (Internet Message Access Protocol)
  - früher: Interactive Mail Access Protocol

MIME

- Zweck: Daten austauschen
- definiert
  - verschiedene Header
  - Typen für Inhalte
  - Anzeigeoptionen

Header

- `MIME-Version: 1.0`
- `Content-Type: <toplevel>/<subtype>`
- `Content-Transfer-Encoding: <encoding>`
- `Content-Disposition: <type>[(; <param>)*]`

Content-Type

- `text`
  - `plain`, `html`, `css`,...
- `application`
  - `octet-stream`, `pdf`, `xml`, `json`, `javascript`,...
- `audio`
  - `mpeg`, `ogg`,...
- `image`
  - `png`, `jpeg`, `gif`
- `video`
  - `mp4`, `VP8`, `H264`,...
- `font`
  - `otf`, `ttf`, `woff`, `woff2`,...
- `multipart:` für mehrere Teile
- `message`: für E-Mails
- `example`: nur für Beispiele

Content-Type

- `text/plain` ... ”kgV aller Formate” bei E-Mails!
  - `text/enrichted` und `text/html`
    - $\rightarrow$ Rückwärtskompatiblität
    - $\rightarrow$ unfreundliche Reaktionen von Empfängern
  - aber...
    - Problem bei der Formatierung von Zeilen und Absätzen!

”Fixed” Text

- `text/plain`
  - Zeilenlänge maximal 998 Zeichen
    - üblicherweise nicht mehr als 78 Zeichen
  - Zeile begrenzt durch CRLF
- Anzeige
  - vorformatiert
    - meist mit Festbreitenschrift
  - wenn Zeilenlänge größer als Anzeige, dann
    - $\rightarrow$ Scrollbar
    - $\rightarrow$ Umbruch
- wird als ”fixed” bezeichnet

Probleme

- Absatz
  - viele Programme verwenden Proportionalschrift und CRLF um Absatz zu kennzeichnen
    - $\rightarrow$ jede ursprüngliche Zeile wird als Absatz formatiert!
- Zeilenlänge
  - Problem bei Antwort-E-Mails, da ursprünglicher Text ”quoted”
  - bei kleinen Displays

Lösung

- Einführung eines neuen Attributes für `test/plain`:
  - `text/plain;format=fixed` (default) oder
  - `text/plain;format=flowed`
  - `text/plain;format=flowed;delsp=yes`
-

Content-Transfer-Encoding

- `7bit`: keine Kodierung, Text, nur ASCII
- `8bit`: keine Kodierung, Text, nicht ASCII, Übertragung mittels ESMTP
- `binary`: keine Kodierung, binärer Inhalt
- `base64`
- `quoted-printable`: Bytes (außerhalb ASCII) zu ASCII
  - Zeichen 127 bis 255: `=XY`
  - `Hello Günter\r\n` → `Hello=20G=C3=BCnter=0D=A`
    - Blanks am Ende *müssen* als `=20` kodiert werden,…
    - alle Zeichen *können* mittels `=XY` kodiert werden

Content-Disposition

- Type
  - `inline`
    - sofort anzeigen
  - `attachment`
    - nicht automatisch anzeigen
    - HTTP: als Download
- Parameter
  - `filename=<name>`
  - `size=<size>`
  - `...`

SMTP

- relativ einfaches, zustandsbehaftetes Protokoll
- end-to-end Protokoll
- zeichenorientiertes Protokoll
  - Kommandos, Daten
  - als ACII
- TCP, Ports 25, 587
- Aufbau
  - Envelope
  - Headers
  - Body
- Ursprünglich: keine Authentifizierung!

Vorgang

1. MUA übergibt an MSA
   - MUA … Mail User Agent
   - MSA … Mail Submission Agent
     - Port 587
     - akzeptiert nur E-Mails berechtigter Benutzer und standardkonforme Aufbereitung (Schnittstelle zum UA!)
   - $\rightarrow$ DNS mittels MX Record
2. MSA übergibt an (lokalen) MTA
   - MTA … Mail Transfer Agent
     - Port 25
     - MSA und MTA oft eine SW!
3. lokaler MTA baut Verbindung zu entfernten MTA auf
   - end-to-end!
   - aber auch über mehrere Hops (Relays, Gateways)

Vorgang – 2

4. entfernter MTA liefert an MDA
   - MDA … Mail Delivery Agent
5. MDA
   - stellt E-Mail in Mailbox des Empfängers
     - 2 Formate: mbox, Maildir
   - weitere Aufgaben: filtern (Spam), in Folder einordnen
6. MRA (optional)
   - MRA … Mail Retrieval Agent
   - greift auf entfernte Mailbox zu
     - z.B. über IAMP oder POP3
   - und stellt E-Mail in lokale Mailbox
     - (mittels eines lokalen MDA)
7. MUA greift auf Mailbox des Empfängers zu
   - Alternative: Zugriff über POP3 oder IMAP

Protokoll

- Kommandos
  - HELO client-hostname $\rightarrow$ Reply: 250
  - MAIL FROM:<source-address> $\rightarrow$ Reply: 250
  - RCPT TO:<dest-address> $\rightarrow$ Reply: 250
  - DATA (endet mit einem Punkt ”.” in eigener Zeile) $\rightarrow$ Reply: 354,250
  - QUIT $\rightarrow$ Reply: 221
- Reply - Codes:
  - 220 <domain> ready
  - 250 Angeforderte Aktion ok und fertig
  - 251 Benutzer nicht lokal; weitergeleitet zu <…>
  - 354 Maileingabe starten; mit <CR><LF> . <CR><LF> beenden
  - 551 Benutzer nicht lokal; bitte <…> versuchen
- Envelope (Umschlag) wird vom MTA zur Auslieferung der E-Mail verwendet.

Beispiel

```
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost. Escape character is '^]'
220 rom.com ESMTP Postfix
>>>helo gallien.com
250 gallien.com
>>>mail from:<asterix@dorf.gallien.com>
250 Ok
>>>rcpt to:<caesar@rom.com>
250 Ok
>>>data 354 End data with <CR><LF>.<CR><LF>
>>>Hi Julius!
>>>.
250 Ok: queued as BB6B9B8245
>>>quit 221 Bye
```

Protokoll – 2

- SMTP ist ASCII…
- ESMTP (Extended SMTP)
  - EHLO anstatt HELO
  - Server teilt Erweiterungen in Antwort mit, z.B.:
    - `8BITMIME` … 8 Bit-Übertragung
    - `AUTH` … SMTP AUTH
    - `STARTTLS` … Umschalten auf TLS
    - `SMTPUTF8` … UTF-8 in Header und Mailbox
    - …

Authentifizierung

- POP before SMTP…
- SMTP Authentication
  - `PLAIN` … in Klartext (Base64)
  - `DIGEST-MD5` … wie in HTTP
- Authentifizierung der MTAs
  -

Envelope und Header

- Envelope (vom MTA)
  - MAIL FROM:<gk@foxl.htlwrn.ac.at>
  - RCPT TO:<ko@htlwrn.ac.at>
- Headers (vom UA), Beispiele:
  - Received-By: mail.htlwrn.ac.at
  - Delieverd-To: ko@htlwrn.ac.at
  - Date: Wed, 13 Aug 2003 10:54:17 +0200 (CEST)
  - From: gk@foxl.htlwrn.ac.at
  - To: ko@htlwrn.ac.at
  - Reply-To: ko@htlwrn.ac.at
  - Subject: bla,bla
  - Header, die mit X− beginnen, sind benutzerdefinierte Felder (z.B. X-Phone, X-Mailer,…)

Relay-Prinzip

- Konfiguration eines MTA

Content-Type: multipart

- mixed
- alternative

Multipart – 2

```
From: Max Mustermann <max@muster-mann.at>
To: Mini Musterfrau <mini@muster-frau.at>
Date: Mon, 27 Aug 2007 09:41:09 +0200 (CEST)
Subject: Multipart E-Mail mit mehreren alternativen Darstellungen
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=trennzeichen

--trennzeichen
Content-Type: text/plain; charset=us-ascii

Text-Version...

--trennzeichen
Content-Type: text/html; charset=utf-8

HTML-Version...

--trennzeichen
Content-Type: application/pdf
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=”mail.pdf”

base64 kodierte PDF-Version

--trennzeichen--
```

Nicht-ASCII in Headers?

- ASCII Zeichen sind ein MUSS
- $\rightarrow$ encoded words
  - `=? charset ? encoding ? encoded text?=`
  - Bsp: `=?iso-8859-1?q?this=20is=20some=20text?=`
    - `q` ... `quoted-printable`
    - `b` ... `base64`
    - da kein Leerzeichen erlaubt!

POP3

- Zugriff auf entfernte Mailboxen
- textorientiert, zustandsorientiert
- TCP, Port 110
- Daten werden auf Client geladen
  - und in Abhängigkeit der Einstellungen am Server gelöscht
- Vorteil
  - offline

IMAP

- Version 4: IMAPv4
- textorientiert, zustandsorientiert
- TCP, Port 143
- Vergleich zu POP3
  - Daten bleiben (üblicherweise) am Server
    - Clients können lokale Kopie anlegen $\rightarrow$ offline…
  - Flags, wie z.B. `seen`, `answered`, `deleted` und benutzerdefinierte Flags werden am Server verwaltet
  - Server verwaltet Folder: herunterladen, speichern, verschieben von E-Mails
  - Suchen am Server! $\rightarrow$ ”Bandbreite”, Leistung am Server vs. Client
  - mehr Funktionen $\rightarrow$ komplexeres Protokoll und komplexere Implementierung (Client und Server)

Punkt-to-Punkt Verschlüsselung

- direkt
  - SMTPS: Port 465
  - POP3S: Port 995
  - IMAPS: Port 993
- STARTTLS: modernere Variante
  - zuerst ”normale” Verbindung
  - Vorteile
    - Verhandlung über Verschlüsselung möglich
    - keine neue Verbindung zu anderen Port notwendig
  - Nachteil
    - MITM möglich
    - UA bieten oft ”TLS wenn möglich” an $\rightarrow$ u.U. unverschlüsselt
    - Wenn UA STARTTLS nicht kennt, dann wird Kennwort u.U. im Klartext gesendet

Software

- MUA
  - Web-based: GMail, Mailpile, Roundcube,…
  - Applikation
    - Kommandozeilen-basiert: msmtp, sendmail,…
    - text-basiert: Alpine, Elm, Mutt, mu4e,…
    - graphisch: Thunderbird, Outlook, Claws Mail,…
- MTA, MSA
  - Postfix, Exim, qmail, Sendmail, MS Exchange, IBM Notes,…
- MDA
  - maildrop, procmail, sendmail,…
- MRA
  - einfach: fetchmail, getmail
  - mit Synchronisation: isync, OfflineIMAP,…
- POP3 und IMAP
  - Dovecot, Citadel, Cyrus (nur IMAP), MS Exchange, IBM Notes,…