E-Mail Protokolle

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Ziele und Einordnung
- E-Mail - Übersicht und Nachrichtenformat
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- IMAP - Internet Message Access Protocol
- Zusammenfassung

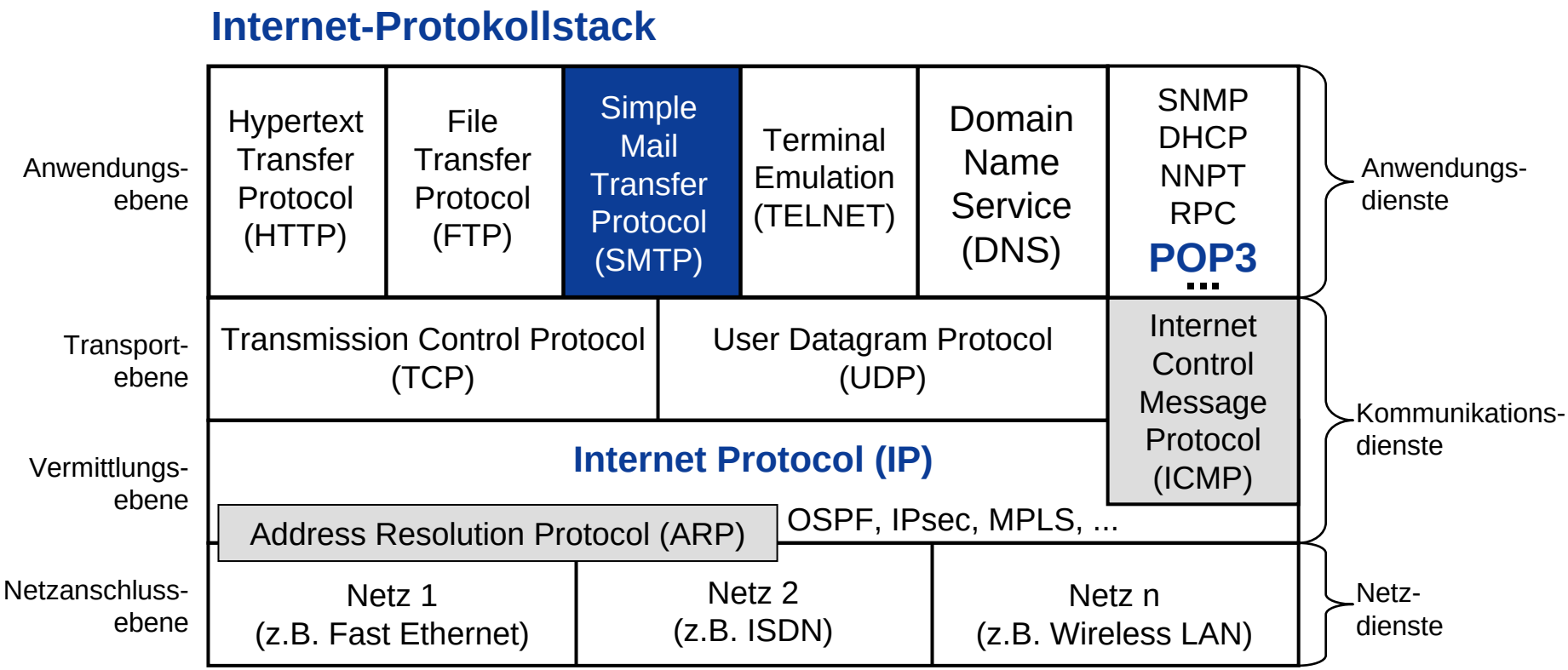
Inhalt

- **Ziele und Einordnung**
- E-Mail - Übersicht und Nachrichtenformat
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- IMAP - Internet Message Access Protocol
- Zusammenfassung

E-Mail Protokolle
→ Ziele

- Gutes Verständnis für die E-Mail Protokolle
- Erlangen der Kenntnisse über die Aufgaben, Prinzipien, Mechanismen und Gefahren der E-Mail Protokolle
- Gewinnen von praktischen Erfahrungen über die E-Mail-Protokolle mit Hilfe von Protokollanalysen und Statistiken (IAS)

Die Anwendungsebene
→ E-Mail Protokolle - Einordnung



Inhalt

- Ziele und Einordnung
- **E-Mail-Übersicht und Nachrichtenformat**
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- IMAP - Internet Message Access Protocol
- Zusammenfassung

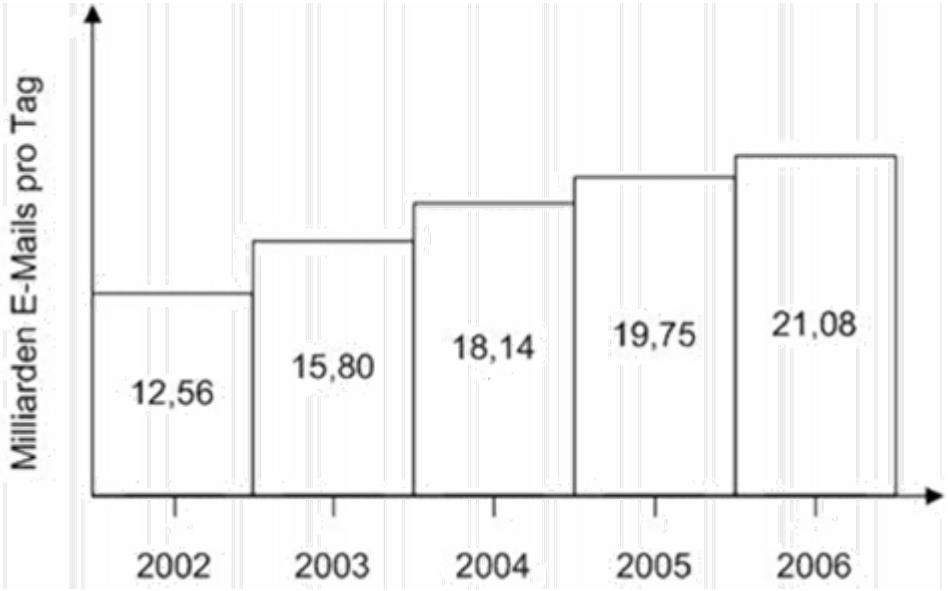
E-Mail Nachrichtenformat
→ Standards und Literatur

RFC 822 Nachrichtenformat

E-Mail
→ Übersicht (1/3)

- **E-Mail, *die elektronische Post*, ist die am häufigsten genutzte Anwendung im Internet!**

- Die IDC-Grafik zeigt die für **geschäftliche Zwecke täglich verschickten E-Mails in Milliarden pro Tag.**

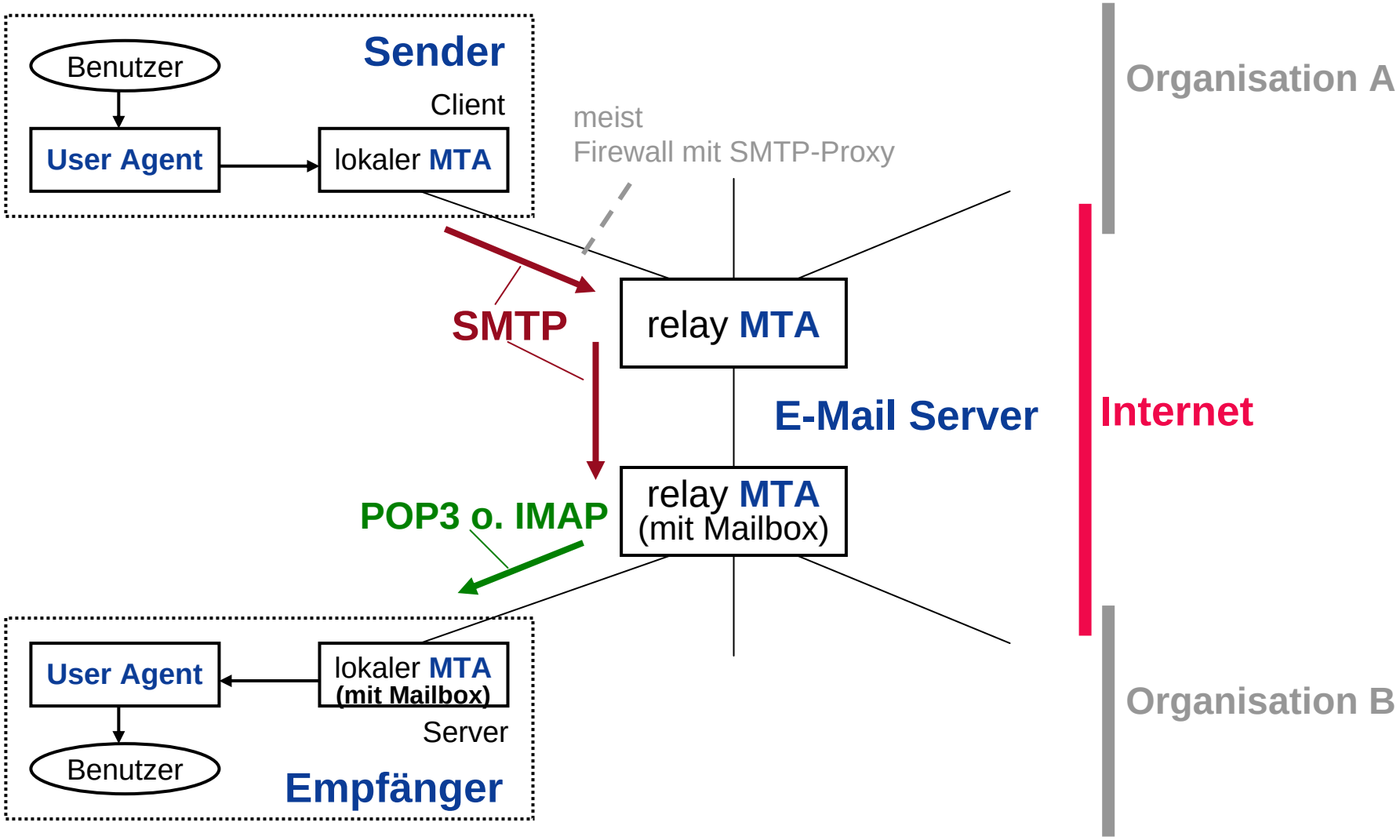


- 1982 wurden die E-Mail Vorschläge in Zusammenhang mit dem ARPANET in den entsprechenden RFCs (821 und 822) veröffentlicht.
- 1984 erstellte die CCITT (heute ITU) die X.400-Empfehlung.
- Nach einem Jahrzehnt des Wettbewerbs wurden die E-Mail-Systeme auf der Grundlage von RFC 822 häufiger benutzt, während die auf X.400 basierenden verschwunden waren.
- **Der Grund für den Erfolg von RFC 822 lag nicht darin, dass das System so gut war, sondern dass X.400 zu komplex war.**

E-Mail
→ Übersicht (2/3)

- Ein E-Mail-System besteht normalerweise aus zwei Teilsystemen:
  - Einem **Benutzeragenten (User Agent - UA)**, mit dem die Benutzer Nachrichten lesen/schreiben und senden/empfangen können.
    - Die User Agents (UA)s sind lokale Programme, die eine auf Benutzerbefehle, Menüs oder Grafik basierende Methode für die Interaktion des Benutzers mit dem E-Mail-System bietet.
  - Einem **Nachrichtenübertragungsagenten (Message Transfer Agent - MTA)**, der die E-Mail zwischen den MTAs transportiert.
    - Der Message Transfer Agent (MTA) ist ein Prozess auf einem Server (Mail-Server), der die E-Mails im System (lokale Organisationen und/oder Internet) befördert.

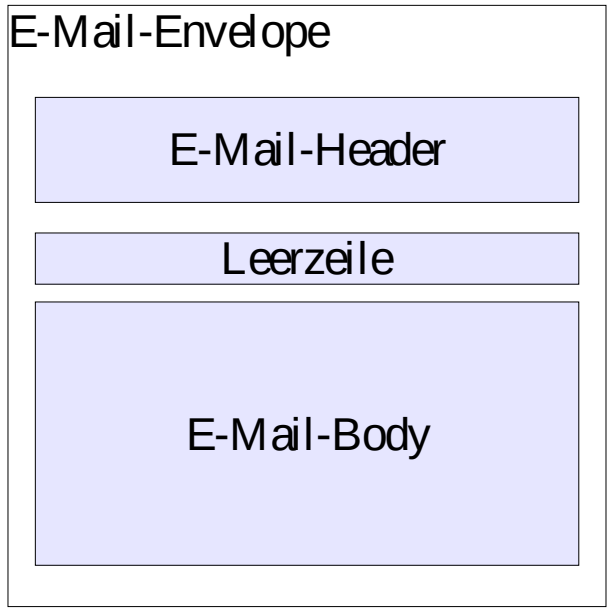
E-Mail
→ Übersicht (3/3)



Hinweis: Die „relay MTAs“ werden im DNS mit MX Records beschrieben

Nachrichtenformat
→ E-Mail-Nachrichten

- Eine E-Mail-Nachricht besteht aus zwei Teilen:
  - Der **Header** enthält hauptsächlich Informationen, die für die Zustellung einer E-Mail wichtig sind, sowie Hinweise für den Empfänger.
  - Der **Body** (Rumpf) enthält den eigentlichen Inhalt bzw. den Text (Bild, Audio, Video, ...) der E-Mail.
- Der Body ist dabei vom Header durch eine Leerzeile getrennt.



- Die RFC 822 legt fest, dass die **E-Mail nur ASCII-Zeichen** enthalten darf (d.h. es stehen nur 7-Bit (0-127) zur Verfügung).
- Damit wird sichergestellt, dass die E-Mails über alle Übertragungskanäle versendet werden können.
- D.h. aber auch, dass alle E-Mails, die einen größeren Zeichensatz benötigen (heute fast alle!), entsprechend kodiert werden müssen!

Nachrichtenformate
→ Nachrichten-Header (1/3)

- Jedes Header-Feld besteht aus einer Zeile mit ASCII-Text, in der der Feldname, ein Doppelpunkt und meist ein Wert stehen.
- Im Normalfall baut der User-Agent (UA) eine E-Mail auf und übergibt sie an den Message Transfer Agent (MTA), der dann einige Header-Felder benutzt, um die E-Mail entsprechend zu übertragen.
- Die wichtigsten Header-Felder sind:

Header	Bedeutung
To:	E-Mail-Adresse(n) des/der primären Empfänger(s)
Cc:	E-Mail-Adresse(n) des/der sekundären Empfänger(s)
Bcc:	E-Mail-Adresse(n) für blinde Kopien an Dritte
From:	Ersteller der Nachricht
Sender:	E-Mail-Adresse des tatsächlichen Absenders
Received:	Zeile, die von jedem Transferagenten auf dem Weg eingefügt wird
Return-Path:	Kann verwendet werden, um einen Pfad zurück zum Absender zu bezeichnen

Nachrichtenformate
→ Nachrichten-Header (2/3)

- **Das Feld An: (To)**
  gibt die DNS-Adresse des primären Empfängers an. Es sind auch mehrere Empfänger zulässig.

- **Das Feld Cc: (Carbon Copy)**
  gibt die Adresse der sekundären Empfänger an. Bei der Zustellung wird zwischen primären und sekundären Empfängern kein Unterschied gemacht. Es handelt sich um einen rein **psychologischen Unterschied**, der für die Benutzer, nicht aber für das E-Mail-System wichtig ist.

- **Das Feld Bcc: (Blind Carbon Copy)**
  hat die gleiche Bedeutung wie das Feld Cc: abgesehen davon, dass die Zeile in allen Kopien, die an die primären und sekundären Empfänger gesendet wird, gelöscht wird. Mit dieser Funktion kann der Benutzer Kopien einer E-Mail an Dritte senden, ohne dass die primären und sekundären Empfänger davon wissen.

Nachrichtenformate
→ Nachrichten-Header (3/3)

- **Die Felder Von: (From) und Absender: (Sender)**
  geben an, wer die E-Mail geschrieben bzw. gesendet hat. Das muss nicht unbedingt die gleiche Person sein (z.B. Chef (Von) - Sekretärin (Absender)). Im Feld Von: ist ein Eintrag erforderlich, während das Feld Absender: weggelassen werden kann, wenn es mit Von: identisch ist.

- **Das Feld Empfänger: (Received)**
  wird vom jedem MTA auf dem Weg eingeführt. In dieser Zeile stehen die Identität des Agenten, Datum und Uhrzeit des Empfangs der E-Mail und weitere Informationen, die Auskunft über **Fehler im Routing-System** geben können.

- **Das Feld Rückweg: (Return-Path)**
  wird vom letzten MTA eingeführt und soll angeben, wie die E-Mail an den Sender zurückgeschickt werden kann.

- Hinweis:
  Diese Informationen werden auch für die SPAM-Analyse verwendet.

Nachrichtenformate
→ Nachrichten-Header (4/3)

- **Weitere Felder für den Nachrichten-Header sind:**

Header	Bedeutung
Date:	Datum und Uhrzeit, wann die Nachricht gesendet wurde
Reply-To:	E-Mail-Adresse, an die Antworten gesendet werden können
Message-Id:	Eindeutige Kennung der Nachricht für eine spätere Bezugnahme
In-Reply-To:	Kennung der Nachricht, der diese Antwort gilt
References:	Andere relevante Nachrichtenkennungen
Keywords:	Vom Benutzer gewählte Schlüsselwörter
Subject:	Kurzer einzeiliger Betreff der Nachricht

- **Das Feld Antwort-an: (Reply-To)**
  wird benutzt, wenn weder der Verfasser (Von) noch der Sender (Absender) der E-Mail die Antwort erhalten wollen.
  Beispiele:
  - → Sender hat zwei E-Mail-Adressen und möchte, dass die Anwort auf die andere Adresse geht
  - → Sekretärin des Marketingleiters sendet eine E-Mail an Kunden, die sich an den Vertriebsleiter wenden sollen

- Alle weiteren Header sind „Private“ und werden i.d.R. mit „X-“ angezeigt.

MIME - Multipurpose Internet Mail Extensions
→ Übersicht

- Bei RFC 822 bestehen E-Mails nur aus Textnachrichten im ASCII-Format.
- Da heute aber die meisten E-Mails andere Typen von Nachrichten übersenden, ist der MIME-Standard (RFC 1341) integriert worden.
- Nach dem Grundkonzept von **MIME** soll das Format RFC 822 weiterhin verwendet werden, jedoch mit **erweiterten Strukturen** für den Nachrichtentext und mit einer Definition der **Kodierungsregeln** für Nicht-ASCII-Nachrichten.
- Ohne von RFC 822 abzuweichen, können MIME-Nachrichten mit den vorhandenen E-Mail-Programmen und -Protokollen übertragen werden.
- MIME definiert fünf neue Nachrichten-Header:

Header	Bedeutung
MIME-Version:	Bezeichnet die MIME-Version
Content-Description:	Vom Benutzer lesbare Zeichenkette, die den Inhalt der Nachricht andeutet
Content-Id:	Eindeutiger Bezeichner
Content-Transfer-Encoding:	Bezeichnet, wie der Nachrichteninhalt für die Übertragung verpackt wurde
Content-Type:	Content-Type:

MIME - Multipurpose Internet Mail Extensions
→ Nachrichten-Header

- **Das Feld MIME-Version**
  informiert den BA, der die E-Mail erhält, dass er es mit einer MIME-Nachricht zu tun hat und welche MIME-Version benutzt wird. Bei E-Mails ohne MIME-Header wird angenommen, dass es sich um ASCII-Text handelt.

- **Das Feld Inhaltsbeschreibung: (Content-Description)**
  ist eine ASCII-Zeichenkette, die auf den Inhalt der Nachricht hinweist.

- **Das Feld Inhaltskennung: (Content-ID)**
  eindeutige Kennung des Inhaltes.

- **Das Feld Übertragungskodierung (Content-Transfer-Encoding)**
  bezeichnet, wie die Nachricht zur Übertragung in einem Netz gekapselt wurde (z.B. **base64** oder **Quoted-Printable**).

- **Das Feld Inhaltstyp: (Content-Type)**
  gibt die Art des Nachrichteninhaltes an (siehe RFC 2045).
  Z.B. Content-Type: video/mpeg

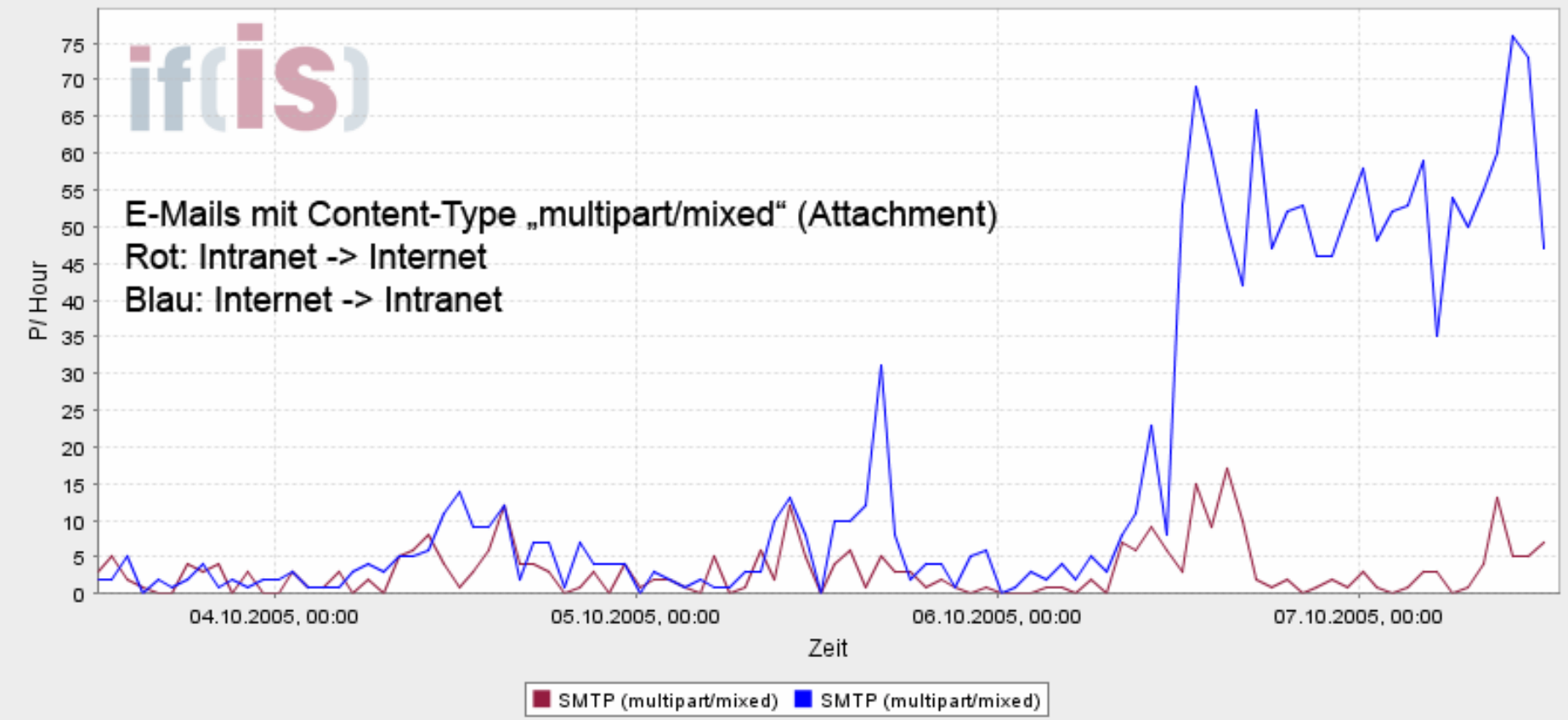
MIME - Multipurpose Internet Mail Extensions
→ base64 Encoding

- Bei dieser Kodierung werden Gruppen von je 24-Bit (3 Byte) in vier 6-Bit-Einheiten zerlegt (4 Byte), und je Einheit wird als zulässiges ASCII-Zeichen übertragen.
- Das heißt, (Binär-)Daten werden durch „**base64 Encoding“ um etwa 33% länger**.
- Die Kodierung lautet „A“ für „0“, „B“ für „1“ usw., gefolgt von den 26 Kleinbuchstaben, den zehn Ziffern sowie „+“ und „/“ für „62“ und „63“.
  - **Code: 0-25 26-51 52-61 62 63**
  - **Zeichen: A-Z a-z 0-9 + /**
- Die Folgen „==„ und „=„ geben an, dass die letzte Gruppe nur 8 bzw. 16 Bit enthielt.
- **Beispiel:**
  - „AAAAAAA“ → „QUFBQUFBQQ==„ (base64 kodiert)

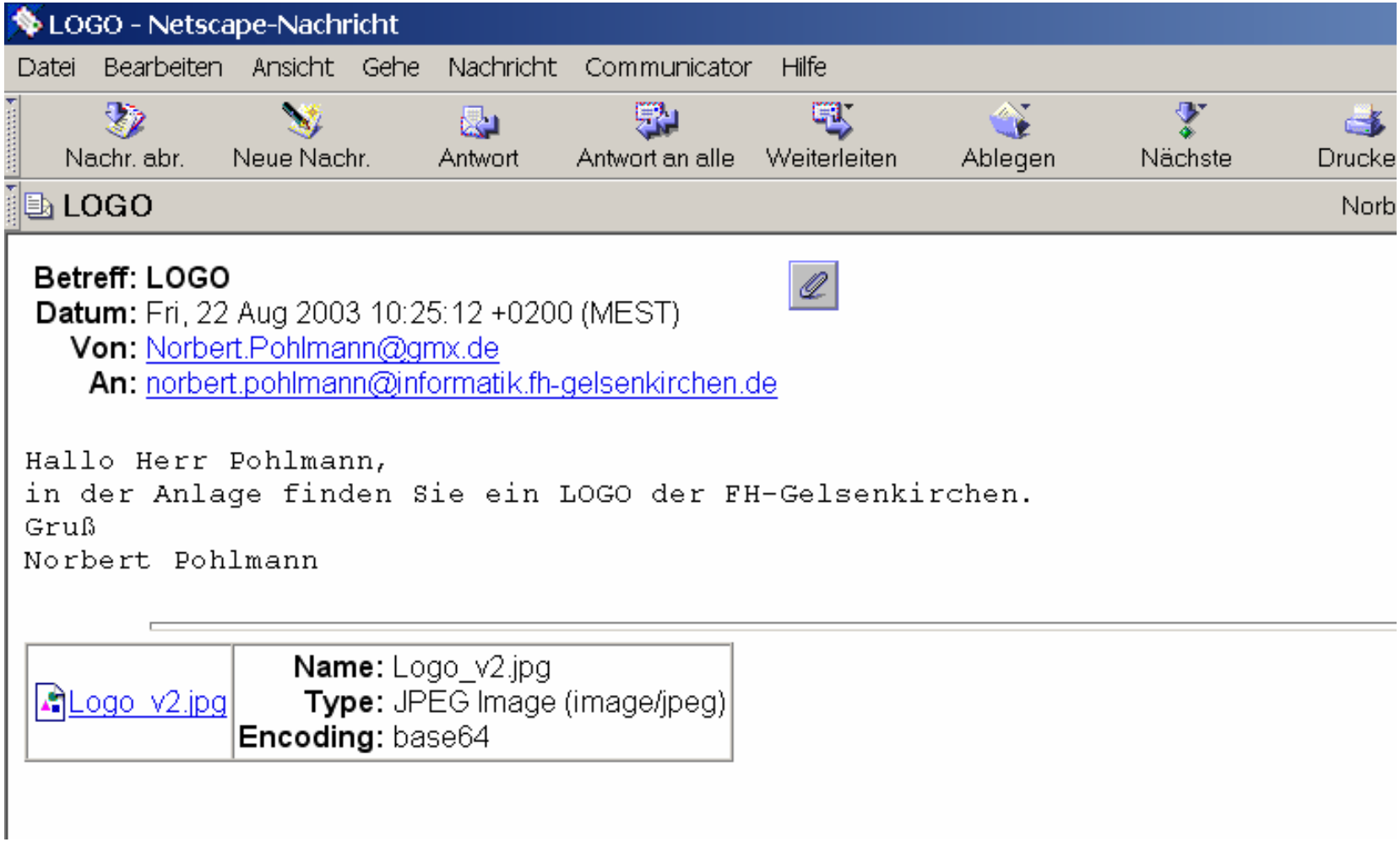
MIME - Multipurpose Internet Mail Extensions
→ MIME-Typen und -Untertypen (Auswahl)

Typ	Untertyp	Beschreibung
Text	Plain	Unformatierter ASCII-Text
	Enriched	ASCII-Text mit einfachen Formatierungen
Image	Gif	Standbild im GIF-Format
	Jpeg	Standbild im JPEG-Format
Audio	Basic	Klangdaten
Video	Mpeg	Laufbilder im MPEG-Format
Application	Octet-stream	Nicht interpretierte Bytefolge
	PostScript	Druckbares Dokument im PostScript-Format
Message	rfc822	MIME-Nachricht nach RFC 822
	Partial	Nachricht wurde zur Übertragung zerlegt
	External-body	Die Nachricht selbst muss vom Netz geholt werden
Multipart	Mixed	Unabhängige Teile in der angegebenen Reihenfolge
	Alternative	Gleiche Nachricht in verschiedenen Formaten
	Parallel	Teile müssen gleichzeitig ausgegeben werden
	Digest	Jeder Teil ist eine vollständige Nachricht nach RFC 822

IAS: FB Informatik
→ Content-Type „multipart/mixed“ (Attachment)



MIME - Multipurpose Internet Mail Extensions
→ Beispiel - Logo E-Mail (1/4) - normale Sichtweise



MIME - Multipurpose Internet Mail Extensions
→ Beispiel - Logo E-Mail (2/4) - Quelltext

```
Return-Path: <Norbert.Pohlmann@gmx.de>
From: Norbert.Pohlmann@gmx.de
Received: by newmail.informatik.fh-gelsenkirchen.de (Postfix)
 id 7951F2BDE8; Fri, 22 Aug 2003 10:29:21 +0200 (CEST)
Delivered-To: norbert.pohlmann@informatik.fh-gelsenkirchen.de
Received: from localhost (newmail [127.0.0.1])
 by newmail.informatik.fh-gelsenkirchen.de (Postfix) with ESMTP id 40ECC2BDF7
 for <norbert.pohlmann@informatik.fh-gelsenkirchen.de>;Fri,22Aug2003 10:29:21+0200(CEST)
Received: from informatik.fh-gelsenkirchen.de (unknown [172.16.17.1])
 by newmail.informatik.fh-gelsenkirchen.de (Postfix) with ESMTP id F23182BDE8
 for <norbert.pohlmann@newmail.informatik.fh-ge.de>;Fri,22Aug2003 10:29:18+0200(CEST)
Received: from mx0.gmx.net (mx0.gmx.de [213.165.64.100])
 by informatik.fh-gelsenkirchen.de (8.11.6/8.11.6) with SMTP id h7M8PJV19332
 for <norbert.pohlmann@informatik.fh-gelsenkirchen.de>;Fri,22Aug2003 10:25:19+0200
Received: (qmail 20910 invoked by uid 0); 22 Aug 2003 08:25:12 -0000
Date: Fri, 22 Aug 2003 10:25:12 +0200 (MEST)
To: norbert.pohlmann@informatik.fh-gelsenkirchen.de
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="========GMXBoundary1397010615407l2"
Subject: LOGO
X-Priority: 1 (Highest)
X-Authenticated-Sender: #0003851597@gmx.net
X-Authenticated-IP: [80.146.125.102]
Message-ID: <13970.1061540712@www54.gmx.net>
X-Mailer: WWW-Mail 1.6 (Global Message Exchange)
X-Flags: 0001
X-Virus-Scanned: by Amavis - > Sophos
X-Mozilla-Status: c001
X-Mozilla-Status2: 00000000
X-UIDL: 8d8ae301adae0bda2fba315be14733ba
```

E-Mail-Server sendet an den eigenen Viren-Scanner

ESMTP-Server von der Firewall

(siehe nslookup - DNS)

X-ABC sind von den Firmen (Mail-Programme, Viren-Scanner, ...) „selbst“ definierte Header

MIME - Multipurpose Internet Mail Extensions
→ Beispiel - Logo E-Mail (3/4) - Quelltext

```
This is a MIME encapsulated multipart message -
please use a MIME-compliant e-mail program to open it.

Dies ist eine mehrteilige Nachricht im MIME-Format -
bitte verwenden Sie zum Lesen ein MIME-konformes Mailprogramm.

--========GMXBoundary139701061540712
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 8bit

Hallo Herr Pohlmann,
in der Anlage finden Sie ein LOGO der FH-Gelsenkirchen.
Gruß
Norbert Pohlmann
--========GMXBoundary139701061540712
Content-Type: image/jpeg; name="Logo_v2.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Logo_v2.jpg"

/9j/4AAQSkZJRgABAQEBLAEsAAD/2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0a
HBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL/2wBDAQkJCQwLDBgNDRgyIRwhMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCAPTCmwDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
```

. . .

Klartext Informationen über die E-Mail; wird nicht angezeigt

Part 1

Die Parts werden durch Boundaries getrennt „--“

Part 2
(1. Teil)

MIME - Multipurpose Internet Mail Extensions
→ Beispiel - Logo E-Mail (4/4) - Quelltext

```
                                . . .
CiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAK
KKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAoo
ooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiii
gAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKA
CiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAK
KKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAoo
ooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigD//2Q==

--========GMXBoundary139701061540712--
```

Part 2
(2. Teil)

- Zusammenfassung:
  - Die Datei „Logo_v2.ipg“ ist 105 KBtye groß, nach der „base64-Kodierung“ ist der E-Mail-Teil 141 KBtye groß (34,28 % mehr!).

MIME - Multipurpose Internet Mail Extensions
→ Beispiel: HGI - E-Mail (Teile des Headers)

```
Return-Path:hgi-news-bounces+norbert.pohlmann=informatik.fh-gelsenkirchen.de@lists.ruhr-uni-boc
Received: by newmail.informatik.fh-gelsenkirchen.de (Postfix)id AE82F2BE06; Mon, 18 Aug 2003
Delivered-To: norbert.pohlmann@informatik.fh-gelsenkirchen.de
Received: from localhost (newmail [127.0.0.1])
        by newmail.informatik.fh-gelsenkirchen.de (Postfix) with ESMTP id 8356D2BE05
        for <norbert.pohlmann@informatik.fh-gelsenkirchen.de>; Mon, 18 Aug 2003 13:27:56
Received: from informatik.fh-gelsenkirchen.de (unknown [172.16.16.1])
        by newmail.informatik.fh-gelsenkirchen.de (Postfix) with ESMTP id AB5DE2BE02
        for <norbert.pohlmann@newmail.informatik.fh-ge.de>; Mon, 18 Aug 2003 13:27:54)
Received: from sunu007.rz.ruhr-uni-bochum.de (sunu007.rz.ruhr-uni-bochum.de [134.147.64.14])
        by informatik.fh-gelsenkirchen.de (8.11.6/8.11.6) with SMTP id h7IBNd711276
        for <norbert.pohlmann@informatik.fh-gelsenkirchen.de>; Mon, 18 Aug 2003 13:23:40
Received: from mailhost.rz.ruhr-uni-bochum.de(HELO sunu007.rz.ruhr-uni-bochum.de)(134.147.64.6)
        by mailhost.rz.ruhr-uni-bochum.de with SMTP; 18 Aug 2003 11:23:39 -0000
Delivered-To: mailman-hgi-news@lists.ruhr-uni-bochum.de
Received: from gierlichs@hgi.ruhr-uni-bochum.de by mailhost with
        qmail-scanner-1.00 (uvscan: v4.2.40/v4285. . Clean. Processed
        in 0.74282 secs); 18 Aug 2003 11:23:35 -0000
Received: from rechnerraum.itsc.ruhr-uni-bochum.de (HELO
        itsc.ruhr-uni-bochum.de) (134.147.19.199)
        by mi-1.rz.ruhr-uni-bochum.de with SMTP; 18 Aug 2003 11:23:34 -0000
Received: from hgi3 (hgi3.itsc.ruhr-uni-bochum.de [134.147.19.213])
        by itsc.ruhr-uni-bochum.de (8.11.6/8.11.6) with ESMTP id h7IBNV001507
        for <hgi-news@lists.ruhr-uni-bochum.de>; Mon, 18 Aug 2003 13:23:31 +0200
To: <hgi-news@lists.ruhr-uni-bochum.de>
Date: Mon, 18 Aug 2003 13:23:33 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;    boundary="----=_NextPart_000_0007_01C3658B.EC4D6320"
From: hgi-news@lists.ruhr-uni-bochum.de
Subject: [HGI-News] Ausgabe 3
Reply-To: info@hgi.ruhr-uni-bochum.de
Sender: hgi-news-bounces+norbert.pohlmann=informatik.fh-gelsenkirchen.de@lists.ruhr-uni-bochum.
```

Inhalt

- Ziele und Einordnung
- E-Mail - Übersicht und Nachrichtenformat
- **SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)**
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- IMAP - Internet Message Access Protocol
- Zusammenfassung

SMTP - Simple Mail Transfer Protokoll
→ Standards und Literatur

RFC 821	Übertragungsprotokoll (SMTP) - 1982
RFC 2821	Übertragungsprotokoll (SMTP) - 2001

SMTP - Simple Mail Transfer Protokoll

- Im Internet wird eine E-Mail zugestellt, indem die Quelle eine TCP-Verbindung zu **Port 25** des Ziels aufbaut.
- Das Abhören dieses Ports übernimmt ein E-Mail-Dämon, der SMTP (Simple Mail Transfer Protocol) spricht.
- Dieser Dämon nimmt ankommende Verbindungen an und kopiert E-Mails in die entsprechenden Mailboxen.
- Nach dem Aufbau der TCP-Verbindung zu Port 25 wartet der sendende Rechner (Client), bis der empfangende Rechner (Server) zuerst mit der Kommunikation beginnt.
- Der Server beginnt durch Aussenden einer Textzeile, durch die er sich identifiziert und mitteilt, ob er E-Mails annehmen kann (HELO o. EHLO).
- Ist der Server bereit, E-Mails entgegenzunehmen, kündigt der Client an, von wem die E-Mail kommt und an wen sie gerichtet ist.
- Existiert der Empfänger am Ziel, gibt der Server dem Client das Startzeichen zum Senden.

SMTP - Simple Mail Transfer Protokoll

- Dann sendet der Client die E-Mail, und der Server bestätigt sie.
- Sind mehrere E-Mails zu versenden, werden sie nacheinander übertragen.
- Wurden die E-Mails in beide Richtungen ausgetauscht, wird die Verbindung freigegeben.

SMTP - Simple Mail Transfer Protokoll
→ SMTP-Kommandos - Requests

Kommandos	Beschreibung
HELO oder EHLO	Eine Art Begrüßung (Hello), in welcher der Client dem Server seine Identität in Form des Domain Names mitteilt. EHLO: Extended SMTP oder ESMTP
MAIL FROM	Einleitung der Übertragung einer E-Mail, enthält die Adresse des Absenders als Parameter
RCPT TO	Festlegung der Empfänger-Adresse(n)
DATA	Einleitung der Übertragung der eigentlichen E-Mail
QUIT	Beendung der Verbindung wird eingeleitet
RSET	Zurücksetzung der Verbindung; bereits eingegebene Daten werden verworfen (Rest)
VRFY	Überprüft, ob eine bestimmte Adresse dem Server als gültiger Empfänger bekannt ist (Verify)
EXPN	Auflösung einer Mailing-Liste, enthält die Adresse, die aufgelöst werden soll, als Parameter
HELP	Ruft Informationen zu dem als Parameter angegebenen Befehl auf
NOOP	Löst nur eine kurze Antwort als Lebenszeichen eine OK-Nachricht des Servers aus; keine weitere Wirkung (No Operation)
TURN	Vertauschung der Client-Server-Rollen: ermöglicht den Versand von E-Mails in die Richtung ohne erneuten Verbindungsaufbau

SMTP - Simple Mail Transfer Protokoll
→ SMTP-Antworten - Response

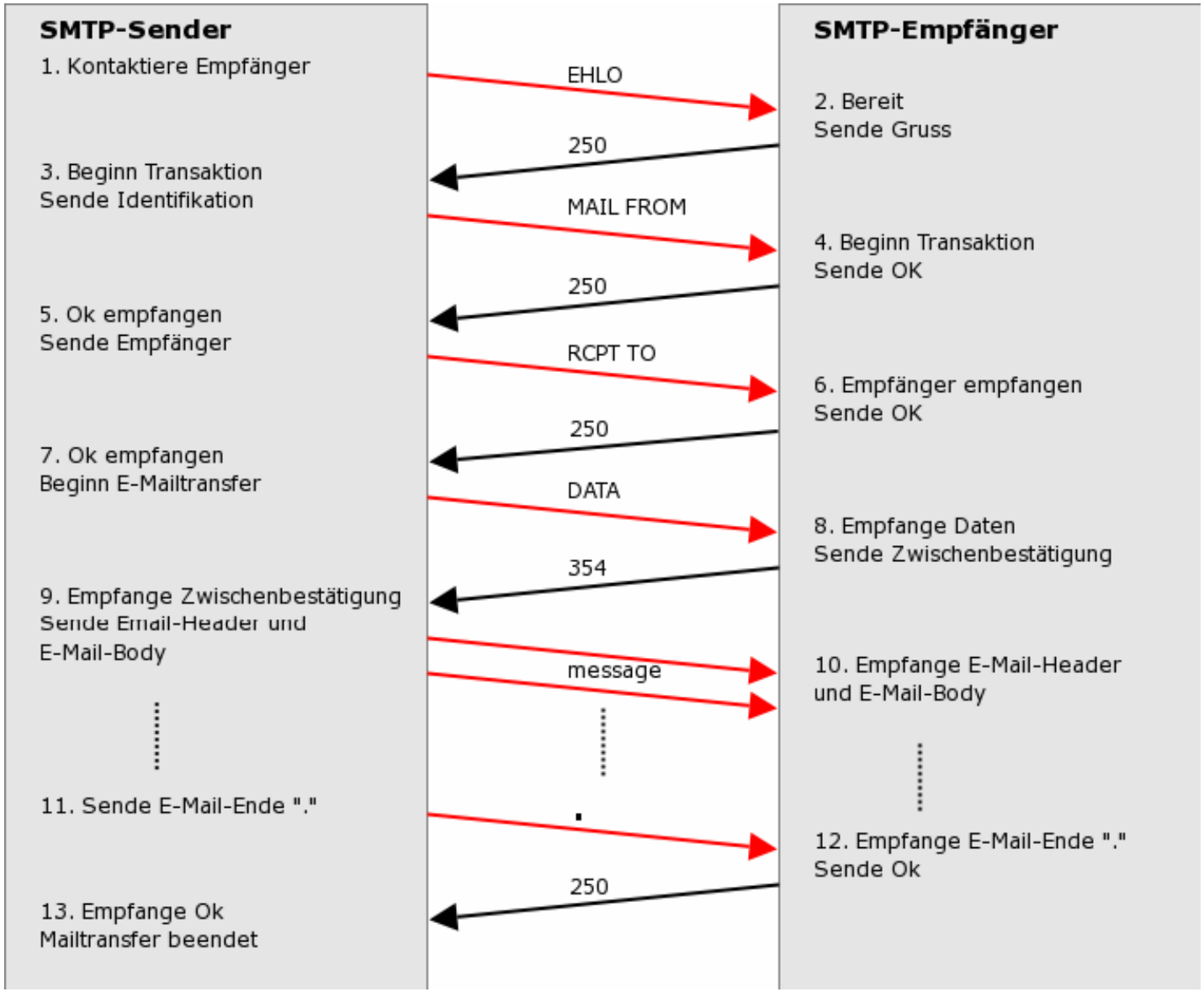
- Dreistellige ASCII-Zahl, optionale Kommentare, <CR><LF>
  - 1yz Positiver Beginn eines Kommandos. Weitere Eingabe erforderlich
  - 2yz Positive Beendigung eines Kommandos. Weitere Kommandos möglich
  - 3yz Positiver Zwischenzustand, aber zusätzliches Kommando erforderlich
  - 4yz Kommando nicht erfolgreich ausgeführt, Wiederholung möglich
  - 5yz Definitives Problem; endgültig nicht erfolgreich

  - x0z Syntaxfehler
  - x1z Allgemeine Information
  - x2z betrifft den Verbindungszustand
  - x3z nicht spezifiziert
  - x4z nicht spezifiziert
  - x5z Statusmeldung

  - z zusätzliche Statuskennung

- Beispiele:
  - 220 alles „ok“, Verbindung hergestellt, Server ist bereit
  - 250 alles „ok“, Kommando ausgeführt
  - 221 Server beendet die Verbindung

SMTP - Simple Mail Transfer Protokoll
→ Ablauf

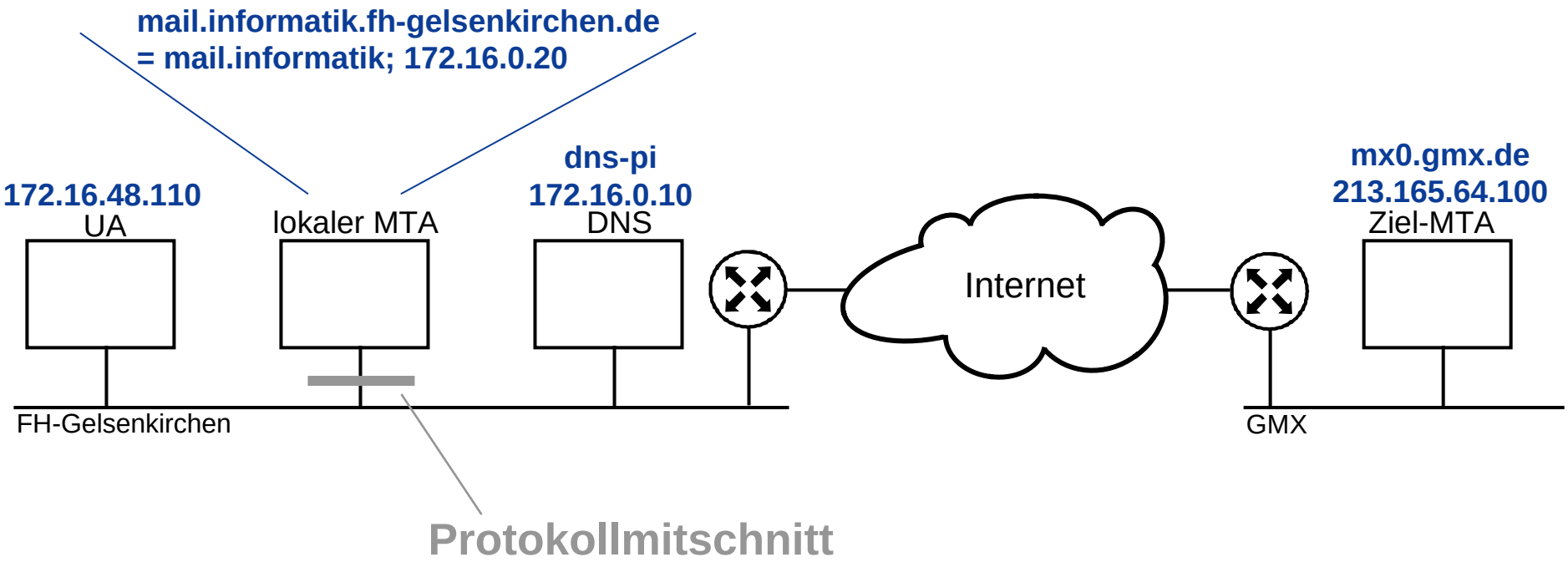


SMTP - Simple Mail Transfer Protokoll
→ Endzustellung

- SMTP geht davon aus, dass alle Benutzer an Rechnern arbeiten, die das Senden und Empfangen von E-Mails zu jeder Zeit unterstützen.
- Bei SMTP wird die E-Mail zugestellt, indem der Sender eine TCP-Verbindung mit dem Empfänger errichtet und dann die E-Mail darüber versendet.
- Dieses Modell funktioniert aber nur dann, wenn der Empfänger die ganze Zeit „online“ ist, um TCP-Verbindungen zu akzeptieren.
- Eine Lösung dieses Problems ist, den MTA mit einer Mailbox-Funktion zu erweitern, die es möglich macht, rund um die Uhr E-Mails für die Benutzer anzunehmen.
- Der Benutzer muss dann, wenn er „online“ ist mit einem Protokoll (POP3, IMAP, ...) die Mailbox kontaktieren, um die Mails „abzurufen“.

SMTP-Protokollmitschnitt

SMTP - Simple Mail Transfer Protokoll
→ Beispiel: Versenden einer E-Mail (UA an Ziel-MTA)



SMTP - Simple Mail Transfer Protokoll
→ Beispiel: Kommunikation UA und lokaler MTA (1/2)

Die Sicherheitsfunktionen sind nicht implementiert!

```
No Time       Source            Destination       Proto.Info
 1 0.000000   172.16.48.110     mail.informatik   TCP   2235 > smtp [SYN] Seq=1577606857 Ack=0 Win=64240 Len=0
 2 0.001015   mail.informatik   172.16.48.110     TCP   smtp > 2235 [SYN, ACK] Seq=3166096652 Ack=1577606858 Win=16368 Len=0
 3 0.001936   172.16.48.110     mail.informatik   TCP   2235 > smtp [ACK] Seq=1577606858 Ack=3166096653 Win=64240 Len=0
```

Aufbau (TCP) vom UA zum lokalen MTA

```
 4 0.013295   mail.informatik   dns-pi            DNS   Standard query PTR 110.48.16.172.in-addr.arpa
 5 0.015908   dns-pi            mail.informatik   DNS   Standard query response, Server failure
```

lokalen MTA versucht den DNS-Name vom UA zu bestimmen

```
 6 0.272494   mail.informatik   172.16.48.110     TCP   26977 > auth [SYN] Seq=1896947650 Ack=0 Win=512 Len=0
 7 0.273258   172.16.48.110     mail.informatik   TCP   auth > 26977 [RST, ACK] Seq=0 Ack=1896947651 Win=0 Len=0
```

lokalen MTA versucht eine Authentikation mit dem UA

```
 8 0.307631   mail.informatik   172.16.48.110     SMTP  Response: 220 mail.informatik.fh-ge.de ESMTP Sendmail 8.8.8/8.8.8;
 9 0.319429   172.16.48.110     mail.informatik   SMTP  Command: EHLO informatik.fh-gelsenkirchen.de
10 0.337195   mail.informatik   172.16.48.110     TCP   smtp > 2235 [ACK] Seq=3166096742 Ack=1577606895 Win=16368 Len=0
11 0.340529   mail.informatik   172.16.48.110     SMTP  Response: 250-mail.informatik.fh-ge.de Hello,pleased to meet you
```

lokalen MTA ist zum Empfang einer E-Mail bereit

```
12 0.360382   172.16.48.110     mail.informatik   SMTP  Command: MAIL FROM:<dirk.bugzel@informatik.fh-gelsenkirchen.de>
13 0.377245   mail.informatik   172.16.48.110     TCP   smtp > 2235 [ACK] Seq=3166096897 Ack=1577606951 Win=16368 Len=0
```

Absender wird übertragen

```
14 0.531983   mail.informatik   dns-pi            DNS   Standard query ANY informatik.fh-gelsenkirchen.de
15 0.540008   dns-pi            mail.informatik   DNS   Standard query ANY informatik.fh-gelsenkirchen.de
```

Lokaler MTA holt sich Info. über die Absenderdomäne

```
16 0.619924   mail.informatik   172.16.48.110     SMTP  Response: 250 <dirk.bugzel@informatik.fh-gelsenkirchen.de>... Sender ok
```

Lokaler MTA akzeptiert den Absender

```
17 0.650569   172.16.48.110     mail.informatik   SMTP  Command: RCPT TO:<dirk.bugzel@gmx.de>
```

Empfänger wird übertragen

```
18 0.654453   mail.informatik   dns-pi            DNS   Standard query ANY gmx.de
19 0.663681   dns-pi            mail.informatik   DNS   Standard query response MX10 mx0.gmx.de MX10 mx0.gmx.net A213.165.65.100
                                                         NS ns.schlund.de NS dns.gmx.net
```

Lokaler MTA holt sich Info. über die Empfängerdomäne

```
20 0.667189   mail.informatik   172.16.48.110     TCP   smtp > 2235 [ACK] Seq=3166096960 Ack=1577606981 Win=16368 Len=0

21 0.689855   mail.informatik   172.16.48.110     SMTP  Response: 250 <dirk.bugzel@gmx.de>... Recipient ok
```

Lokaler MTA akzeptiert den Empfänger

SMTP - Simple Mail Transfer Protokoll
→ Beispiel: Kommunikation UA und lokaler MTA (2/2)

No	Time	Source	Destination	Proto.	Info
22	0.731247	172.16.48.110	mail.informatik	SMTP	Command: DATA
23	0.733506	mail.informatik	172.16.48.110	SMTP	Response: 354 Enter mail, end with "." on a line by itself
					Einleitung der E-Mail Übertragung
24	0.776828	172.16.48.110	mail.informatik	SMTP	Message Body
					E-Mail Übertragung
25	**0.794558**	**mail.informatik**	**172.16.16.8**	**Syslog**	**MAIL.INFO: sendmail[677]: MAA00677: fro...**
26	0.797178	mail.informatik	172.16.48.110	TCP	smtp > 2235 [ACK] Seq=3166097052 Ack=1577607462 Win=16368 Len=0
27	0.817765	mail.informatik	172.16.48.110	SMTP	Response: 250 MAA00677 Message accepted for delivery
28	0.839527	172.16.48.110	mail.informatik	SMTP	Message Body (Quit)
29	0.841124	mail.informatik	172.16.48.110	SMTP	Response: 221 mail.informatik.fh-ge.de closing connection
					Positive Beendigung der E-Mail Übertragung
30	0.842124	mail.informatik	172.16.48.110	TCP	smtp > 2235 [FIN, ACK] Seq=3166097145 Ack=1577607468 Win=16368 Len=0
31	0.842739	172.16.48.110	mail.informatik	TCP	2235 > smtp [ACK] Seq=1577607468 Ack=3166097146 Win=63748 Len=0
32	0.879880	172.16.48.110	mail.informatik	TCP	2235 > smtp [FIN, ACK] Seq=1577607468 Ack=3166097146 Win=63748 Len=0
33	0.880540	mail.informatik	172.16.48.110	TCP	smtp > 2235 [ACK] Seq=3166097146 Ack=1577607469 Win=16367 Len=0
					Abbau (TCP) zwischen UA zum lokalen MTA

SMTP - Simple Mail Transfer Protokoll
→ Beispiel: Kommunikation lokaler MTA und Ziel-MTA (1/2)

```
No Time      Source           Destination      Proto.Info
34 0.889676  mail.informatik  dns-pi           DNS   Standard query MX gmx.de
35 0.896671  dns-pi           mail.informatik  DNS   Standard query response MX 10 mx0.gmx.de MX 10 mx0.gmx.net

36 0.907272  mail.informatik  dns-pi           DNS   Standard query A mx0.gmx.de
37 0.951348  dns-pi           mail.informatik  DNS   Standard query response A 213.165.64.100
```

lokalen MTA fragt nach der ADR des Ziel-MTAs

```
38 0.954606  mail.informatik  mx0.gmx.net      TCP   26978 > smtp [SYN] Seq=78221664 Ack=0 Win=512 Len=0
39 0.973485  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [SYN, ACK] Seq=91041251 Ack=78221665 Win=5840 Len=0
40 0.974047  mail.informatik  mx0.gmx.net      TCP   26978 > smtp [ACK] Seq=78221665 Ack=91041252 Win=16060 Len=0
```

Aufbau (TCP) vom lokalen MTA zum Ziel-MTA

```
41 0.995857  mx0.gmx.net      mail.informatik  SMTP  Response: 220 {mx023-rz3} GMX Mailservices ESMTP
42 0.997744  mail.informatik  mx0.gmx.net      SMTP  Command: EHLO mail.informatik.fh-ge.de
43 1.016120  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [ACK] Seq=91041292 Ack=78221696 Win=5840 Len=0
44 1.016284  mx0.gmx.net      mail.informatik  SMTP  Response: 250-{mx023-rz3} GMX Mailservices
```

Ziel MTA ist zum Empfang einer E-Mail bereit

```
45 1.017769  mail.informatik  mx0.gmx.net      SMTP  Command: MAIL From:<dirk.bugzel@informatik.fh-ge.de>
46 1.040867  mx0.gmx.net      mail.informatik  SMTP  Response: 250 {mx023-rz3} ok
```

Absender wird übertragen und akzepiert

```
47 1.042011  mail.informatik  mx0.gmx.net      SMTP  Command: RCPT To:<dirk.bugzel@gmx.de>
48 1.078882  mx0.gmx.net      mail.informatik  SMTP  Response: 250 {mx023-rz3} ok
```

Empfänger wird übertragen und akzeptiert

Der Ziel-MTA wird sicherlich auch DNS-Anfragen durchführen, die an dieser Stelle nicht zu sehen sind

SMTP - Simple Mail Transfer Protokoll
→ Beispiel: Kommunikation lokaler MTA und Ziel-MTA (2/2)

```
No Time      Source           Destination      Proto.Info
49 1.079978  mail.informatik  mx0.gmx.net      SMTP  Command: DATA
50 1.099217  mx0.gmx.net      mail.informatik  SMTP  Response: 354 {mx023-rz3} Go ahead
```

Einleitung der E-Mail Übertragung

```
51 1.110437  mail.informatik  mx0.gmx.net      SMTP  Message Body
52 1.163234  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [ACK] Seq=91041406 Ack=78222237 Win=6432 Len=0
53 1.163778  mail.informatik  mx0.gmx.net      SMTP  EOM: .
54 1.182223  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [ACK] Seq=91041406 Ack=78222240 Win=6432 Len=0
55 1.195491  mx0.gmx.net      mail.informatik  SMTP  Response: 250 {mx023-rz3} Message accepted

56 1.198549  mail.informatik  172.16.16.8      SyslogMAIL.INFO: sendmail[679]: MAA00677: to=...
```

E-Mail Übertragung

```
57 1.207125  mail.informatik  mx0.gmx.net      TCP   26978 > smtp [ACK] Seq=78222240 Ack=91041440 Win=16060 Len=0

58 1.296972  mail.informatik  mx0.gmx.net      SMTP  Command: QUIT
59 1.315926  mx0.gmx.net      mail.informatik  SMTP  Response: 221 {mx023-rz3} GMX Mailservices
```

Positive Beendigung der E-Mail Übertragung

```
60 1.316022  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [FIN, ACK] Seq=91041474 Ack=78222246 Win=6432 Len=0
61 1.316735  mail.informatik  mx0.gmx.net      TCP   26978 > smtp [ACK] Seq=78222246 Ack=91041475 Win=16060 Len=0

62 1.317422  mail.informatik  mx0.gmx.net      TCP   26978 > smtp [FIN, ACK] Seq=78222246 Ack=91041475 Win=16060 Len=0
63 1.338723  mx0.gmx.net      mail.informatik  TCP   smtp > 26978 [ACK] Seq=91041475 Ack=78222247 Win=6432 Len=0
```

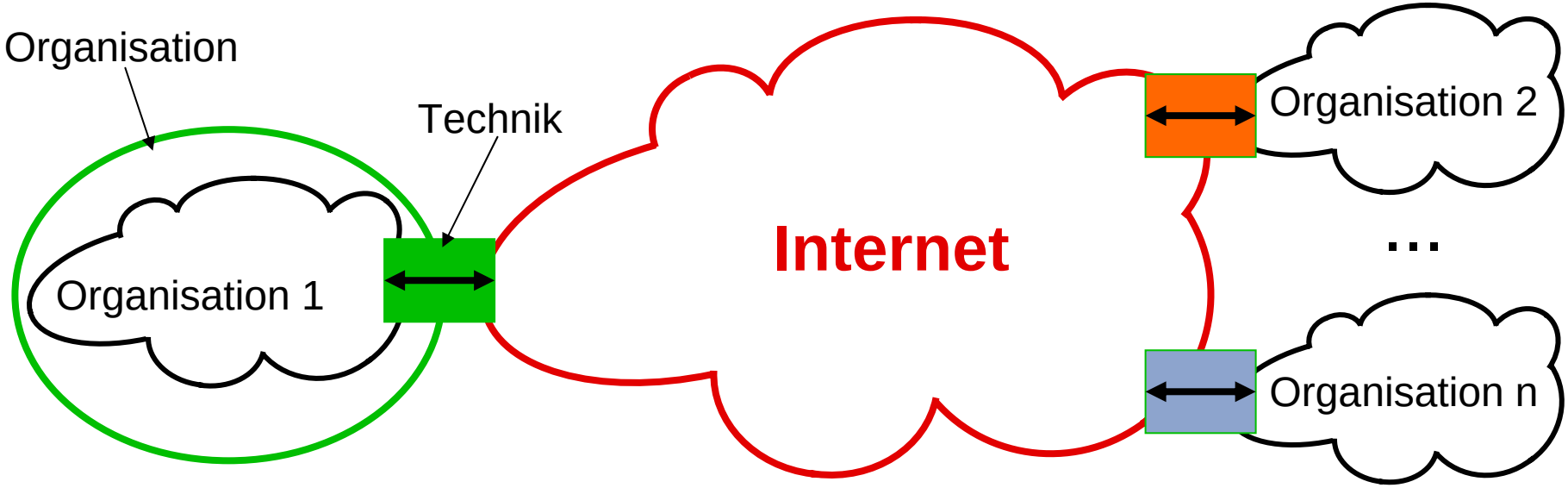
Abbau (TCP) lokalen MTA zum Ziel-MTA

SMTP - Simple Mail Transfer Protokoll
→ Problem SPAM-Mails

- Definition von SPAM
  - **SPAM-Mails sind „unerwünschte“ / „unverlangte“ E-Mails.**
  - **SPiced hAM** - Frühstücksfleich in Dosen

- Besondere Probleme des Internets
  - Das Internet ist ein **offenes System**, jeder kann jedem etwas senden.
  - Der Dienst E-Mail muss **nicht** besonders **bezahlt werden**.
  - Außerdem geht das Internet über alle **geographischen und politischen Grenzen, Gesetze und Kulturen hinaus** und stellt somit eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar.
  - Die Herkunft der SPAM-Mails ist schwer identifizierbar, da die Adressen, mit denen Spammer arbeiten, oftmals nicht existent oder gefälscht sind.

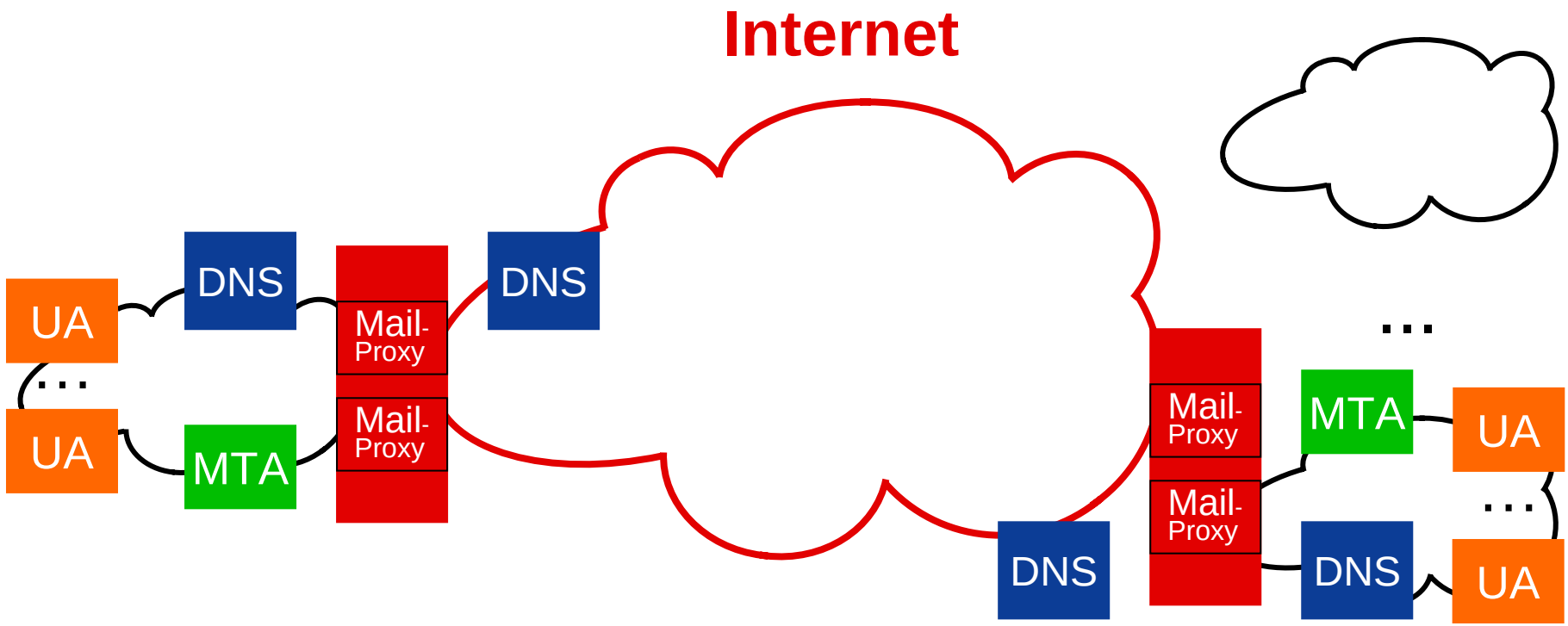
E-Mail im globalem Internet
→ Sichtweise



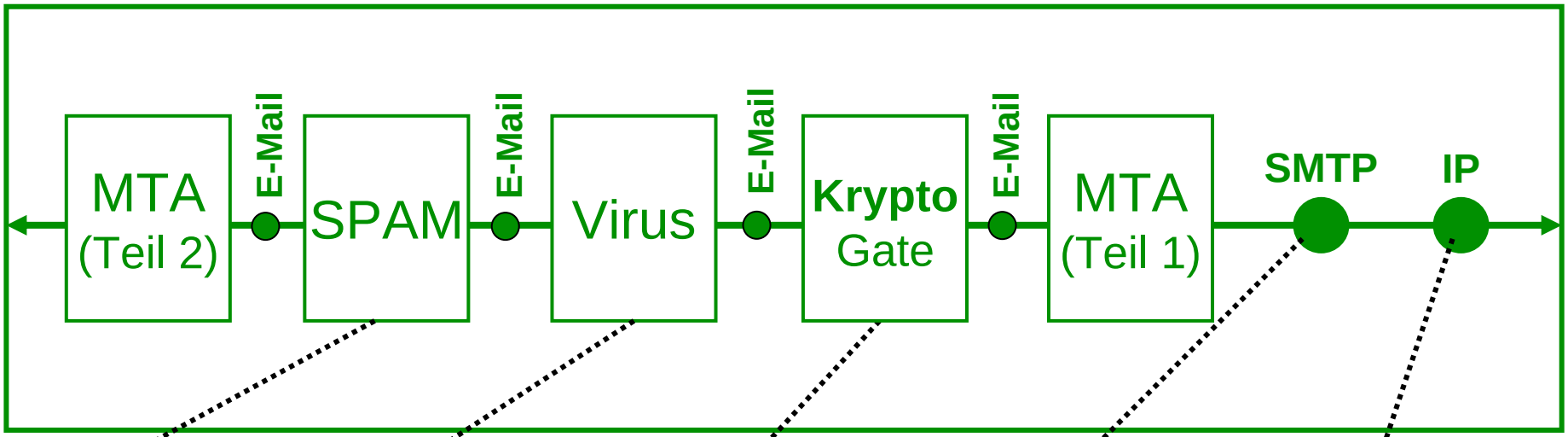
Organisationen

- **Unternehmen**
  (Siemens, Deutsche Bank, usw.)
- **E-Mail-Services Anbieter**
  (Web.de, GMX, Freenet, NetCologne, usw.)
- **ISPs**
  (T-Online, …)

E-Mail im gobalem Internet
→ Beispiel eines Szenario (Unternehmen)



Internetzugang
→ IT-Sicherheitsmaßnahmen in der Praxis



Filter
- Header
- Inhalt
- Hash
- Kombi-nationen
- usw.

10 - 80%

Scanner
- ein oder mehrere
- Updateverfahren
- besondere Mechanismen
- usw.

10 - 50%

- Ent-schlüsselung
- Signatur--überprüfung
- usw.

0 - 5%

- Grey-Liste
- IP ohne Revers DNS (SenderID, ...)
- Existiert ADR?
- usw.

0 - 45%

Black/White List
- Dynamische IP
- Open Relays
- Frequenz-messungen
- usw.

0 - 40%

Wirkung

Inhalt

- Ziele und Einordnung
- E-Mail - Übersicht und Nachrichtenformat
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- **POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)**
- IMAP - Internet Message Access Protocol
- Zusammenfassung

POP3 - Post Office Protocol Version 3
→ Standards und Literatur

RFC 1939 - 1996

POP3 - Post Office Protocol Version 3
→ Übersicht

- POP3 ist ein Protokoll, mit dem der UA den MTA (Mailbox) kontaktieren kann und die E-Mails vom MTA auf den UA kopiert werden können.
- POP3 beginnt, wenn der Benutzer ein Mailprogramm startet.
- Das Mailprogramm (UA) richtet mit dem MTA an Port 110 eine TCP-Verbindung ein.
- Ist eine Verbindung aufgebaut, durchläuft das POP3-Protokoll nacheinander drei Zustände:
  - **Autorisierung**
    Hier findet die Benutzer-Identifizierung und Authentisierung statt
  - **Transaktion**
    In diesem Zustand werden die Operationen zur Bearbeitung der E-Mails ausgeführt.
  - **Aktualisierung**
    In diesem Zustand (nach dem Quit-Kommando) beendet der Server die TCP-Verbindung und führt die angeforderten Änderungen durch.

POP3 - Post Office Protocol Version 3
→ Ablauf

- Während der Autorisierungsphase sendet der Client den Benutzernamen und das Passwort.
- Nach einer erfolgreichen Anmeldung kann der Client das LIST-Kommando senden, durch den der Server die Inhalte der Mailbox mit einer E-Mail pro Zeile auflistet und die Länge der Nachricht angibt.
- Diese Liste wird mit einem Punkt beendet.
- Der Client kann dann die E-Mails mit dem RETR-Kommando abrufen und sie zum Löschen mit dem DELE-Kommando markieren.
- Wurden alle E-Mails abgerufen, ruft der Client das Kommando QUIT auf, um den Transaktionszustand zu beenden und in den Aktualisierungszustand überzugehen.
- Hat der Server alle E-Mails gelöscht, sendet er eine Nachricht und bricht die TCP-Verbindung ab.

POP3 - Post Office Protocol Version 3
→ POP3-Kommandos - Requests

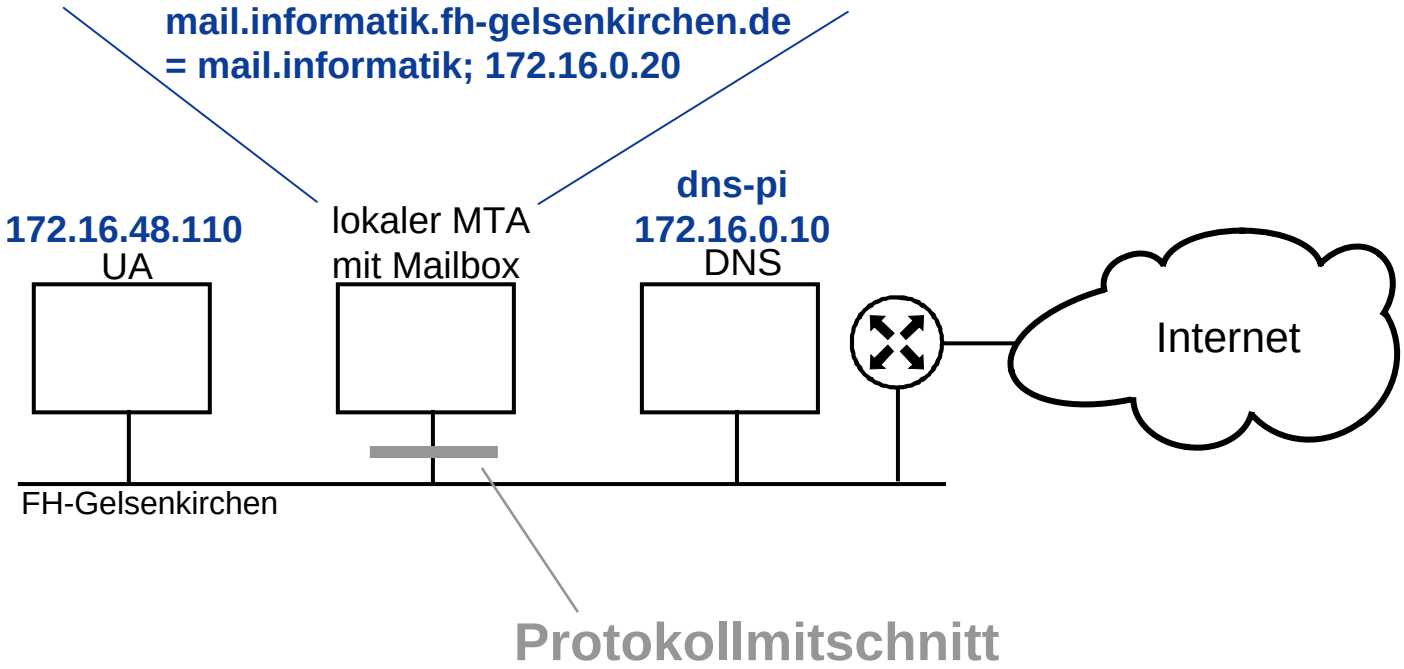
Kommandos	Beschreibung
USER name	Hiermit wird der Name (ID) des Benutzers übertragen
PASS string	Übertragung des Benutzer-Passwortes
QUIT	Beendung der Verbindung wird eingeleitet
STAT	Liefert die Anzahl der gespeicherten E-Mails und die gesamte Größe zurück
LIST [msg]	Liefert die Nummer und die Größe aller E-Mails zurück. Wird als Argument eine Mail-Nummer angegeben, wird nur die Größe dieser Mail ausgegeben
RETR msg	Abruf der E-Mails
DELE msg	Löscht die E-Mails mit der übergebenen Nummer
NOOP	Löst nur eine kurze Antwort als Lebenszeichen eine OK-Nachricht des Servers aus; keine weitere Wirkung (No Operation)
TOP msg n	Optional: Nur Header und die ersten n Zeilen abfragen
RSET	Zurücksetzung der Verbindung; bereits eingegebene Daten werden verworfen (Rest)
UIDL msg	Optional: Einheitliche ID für die E-Mails abfragen

POP3 - Post Office Protocol Version 3
→ POP3-Antworten - Response

- Eine POP3-Response kann 512 Zeichen lang sein.
- Sie besteht aus einem Status Indikator und einer Nachricht im Klartext.
- Es gibt einen positiven („+OK“) und einen negativen („-ERR“) Status Indikator.
- Manche Antworten enthalten weitere Informationen wie, z.B. die Zahl der Nachrichten.

POP3-Protokollmitschnitt

POP3 - Post Office Protocol Version 3
→ Beispiel: Abfrage von E-Mails von der Mailbox



POP3 - Post Office Protocol Version 3
→ Beispiel: Kommunikation UA und lokaler MTA (1/2)

```
No. Time       Source          Destination     Proto.Info
259 48.164070  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [SYN] Seq=2264574574 Ack=0 Win=64240 Len=0
260 48.165025  172.16.0.20     172.16.48.110   TCP   pop3 > 2255 [SYN, ACK] Seq=3468922471 Ack=2264574575 Win=16368 Len=0
261 48.165764  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [ACK] Seq=2264574575 Ack=3468922472 Win=64240 Len=0
```

Aufbau (TCP) vom UA zum lokalen MTA (Mailbox)

```
262 48.691309  172.16.0.20     172.16.48.110   TCP   29312 > auth [SYN] Seq=3870957196 Ack=0 Win=512 Len=0
263 48.692562  172.16.48.110   172.16.0.20     TCP   auth > 29312 [RST, ACK] Seq=0 Ack=3870957197 Win=0 Len=0
```

lokalen MTA versucht eine Authentikation mit dem UA

```
265 48.737842  172.16.0.20     172.16.0.10     DNS   Standard query PTR 110.48.16.172.in-addr.arpa
266 48.740402  172.16.0.10     172.16.0.20     DNS   Standard query response, Server failure
```

lokalen MTA versucht den DNS-Name vom UA zu bestimmen

```
268 48.757444  172.16.0.20     172.16.48.110   POP   Response: +OK QPOP (version2.2)at mail.informatik.fh-ge.de starting.
```

lokalen MTA ist zur Kommunikation bereit

```
269 48.775822  172.16.48.110   172.16.0.20     POP   Request: USER testuser
270 48.777147  172.16.0.20     172.16.48.110   POP   Response: +OK Password required for testuser.
```

Identifikation

```
271 48.798822  172.16.48.110   172.16.0.20     POP   Request: PASS ganzgeheim
272 48.813304  172.16.0.20     172.16.48.110   TCP   pop3 > 2255 [ACK] Seq=3468922573 Ack=2264574605 Win=16368 Len=0
273 48.990856  172.16.0.20     172.16.48.110   POP   Response: +OK testuser has 3 messages (3774 octets).
```

Authentikation

```
274 48.992620  172.16.48.110   172.16.0.20     POP   Request: STAT
275 48.993876  172.16.0.20     172.16.48.110   POP   Response: +OK 3 3774
```

Abruf des Statuses (3 E-Mails; Summe=3774 Byte)

```
276 49.010259  172.16.48.110   172.16.0.20     POP   Request: LIST
277 49.011284  172.16.0.20     172.16.48.110   POP   Response: +OK 3 messages (3774 octets)
278 49.164104  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [ACK] Seq=2264574617 Ack=3468922659 Win=64053 Len=0
279 49.164645  172.16.0.20     172.16.48.110   POP   Continuation
```

Abruf aller E-Mail Informationen (3 E-Mails)

POP3 - Post Office Protocol Version 3
→ Beispiel: Kommunikation UA und lokaler MTA (2/2)

```
No. Time       Source          Destination     Proto.Info
280 49.180147  172.16.48.110   172.16.0.20     POP   Request: UIDL
281 49.181151  172.16.0.20     172.16.48.110   POP   Response: +OK uidl command accepted.
282 49.382839  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [ACK] Seq=2264574623 Ack=3468922714 Win=63998 Len=0
283 49.383545  172.16.0.20     172.16.48.110   POP   Continuation
```

Abfrage der einheitlichen IDs der E-Mail

```
284 49.399626  172.16.48.110   172.16.0.20     POP   Request: RETR 3
285 49.400719  172.16.0.20     172.16.48.110   POP   Response: +OK 1250 octets
286 49.601504  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [ACK] Seq=2264574631 Ack=3468922842 Win=63870 Len=0
287 49.604124  172.16.0.20     172.16.48.110   POP   Continuation
```

Herunterladen der 3 E-Mails

```
288 49.681974  172.16.48.110   172.16.0.20     POP   Request: QUIT
290 49.693200  172.16.0.20     172.16.48.110   TCP   pop3 > 2255 [ACK] Seq=3468924095 Ack=2264574637 Win=16368 Len=0
291 49.702422  172.16.0.20     172.16.48.110   POP   Response: +OK Pop server at mail.informatik.fh-ge.de signing off.
```

Positive Beendigung der Kommunikation

```
292 49.705200  172.16.0.20     172.16.48.110   TCP   pop3 > 2255 [FIN, ACK] Seq=3468924152 Ack=2264574637 Win=16368 Len=0
293 49.706069  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [ACK] Seq=2264574637 Ack=3468924153 Win=64183 Len=0

294 49.735092  172.16.48.110   172.16.0.20     TCP   2255 > pop3 [FIN, ACK] Seq=2264574637 Ack=3468924153 Win=64183 Len=0
295 49.735618  172.16.0.20     172.16.48.110   TCP   pop3 > 2255 [ACK] Seq=3468924153 Ack=2264574638 Win=16367 Len=0
```

Abbau der TCP-Verbindung zwischen UA und lokalem MTA

Hinweis: Die E-Mails sind nicht gelöscht worden!

Inhalt

- Ziele und Einordnung
- E-Mail - Übersicht und Nachrichtenformat
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- **IMAP - Internet Message Access Protocol**
- Zusammenfassung

IMAP - Internet Message Access Protocol
→ Standards und Literatur

RFC 2060 - 1996

IMAP - Internet Message Access Protocol
→ Übersicht

- Alternativ zu POP3 kann auch IMAP4 eingesetzt werden.
- IMAP4 erlaubt es dem Benutzer, auf dem MTA verschiedene Mailboxen zu halten und zu manipulieren.
- Damit können E-Mails an zentraler Stelle verwaltet werden.
- Dadurch empfiehlt sich IMAP besonders dann, wenn von verschiedenen UAs auf die Mail zugegriffen wird.
- IMAP zeigt für jede ausgewählte Mailbox nur Header-Informationen der Mails (Absender, Subject, Datum, Größe, usw.) an.
- Das Herunterladen der Mail muss explizit veranlasst werden.
- Dadurch ist IMAP gerade auch für den Zugriff über langsame Leitungen, wie z.B. Modems, besonders geeignet.

POP3 versus IMAP

Funktion	POP3	IMAP
Protokoll definiert in	RFC 1939	RFC 2060
Verwendeter TCP-Port	110	143
E-Mail gespeichert auf	Benutzer-PC	Server
Lesen von E-Mail	Offline	Online
Erforderliche Verbindungszeit	Viel	Wenig
Belegte Server-Ressourcen	Minimal	Erheblich
Mehrere Mailboxen	Nein	Ja
Wer sichert Mailboxen	Benutzer	ISP
Gut für mobile Benutzer	Nein	Ja
Benutzer hat Kontrolle über Download	Wenig	Sehr viel
Herunterladen von Teilnachrichten	Nein	Ja
Kann die Festplattenkapazität ein Problem werden	Nein	Eventuell im Laufe der Zeit
Einfache Implementierung	Ja	Nein
Verbreiteter Support	Ja	Zunehmend

Inhalt

- Ziele und Einordnung
- E-Mail - Übersicht und Nachrichtenformat
- SMTP - Simple Mail Transfer Protocol (Protokollmitschnitt)
- POP3 - Post Office Protocol Version 3 (Protokollmitschnitt)
- IMAP - Internet Message Access Protocol
- **Zusammenfassung**

E-Mail Protokolle
→ Zusammenfassung

- SMTP ist ein Protokoll mit dem die **E-Mails** zwischen UA-MTA sowie zwischen den MTAs (in Organisationen und im Internet) **befördert** werden.
  - SMTP läuft auf Port 25
- POP3 ist ein Protokoll, mit dem der UA den MTA (Mailbox) kontaktieren kann und die **E-Mails** vom MTA **auf den UA kopiert** werden können.
  - POP3 läuft auf Port 110
- IMAP ist ein Protokoll, das es dem Benutzer erlaubt, auf dem MTA verschiedene Mailboxen zu halten und zu manipulieren. Damit können die **E-Mails zentral verwaltet** werden!
  - IMAP läuft auf Port 143
- **Verhinderung von SPAM-Mails in der Infrastruktur**
  - Die Unternehmen und Provider sollen alles tun, um ihre MTAs und Mail-Clients gegen Missbrauch zu schützen, damit die SPAM-Mails so stark wie nur möglich schon in der Infrastruktur verhindert werden.

E-Mail Protokolle

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen