Digitale Kommunikation und Internetdienste 1

Wintersemester 2004/2005 – Teil 12

Belegnummer Vorlesung: 39 30 02

Übungen: 39 30 05

Jan E. Hennig

AG Rechnernetze und Verteilte Systeme (RVS)
Technische Fakultät
Universität Bielefeld

jhennig@rvs.uni-bielefeld.de

basierend auf den Arbeiten von Michael Blume, Heiko Holtkamp, Marcel Holtmann und I Made Wiryana

Organisatorisches

- vorab: ein frohes neues Jahr!

- Termine für Übungen verlegt:
  - Übung 5 statt am 23./24.12.2004 nun am 06./07.01.2005
  - Übung 6 statt am 06./07.01.2005 nun am 13./14.01.2005

- Klausur am 20.01.2005:
  - es wird eine zusätzliche Frage auf der Klausur angeboten (evtl. auch zwei)
  - wenn passend beantwortet zeigen diese, daß man zusätzliche 15 Stunden über die Veranstaltung hinaus dem Thema gewidmet hat
  - diese 15h bedeuten 0,5 LP und damit könnte man als MGSler 5 LP statt 4,5 LP für diese Veranstaltung bekommen
  - für MIGler gilt dieses Angebot nicht, da sie fixierte 4 LP bekommen und weniger Leistung beweisen müssen, um die Klausur zu bestehen

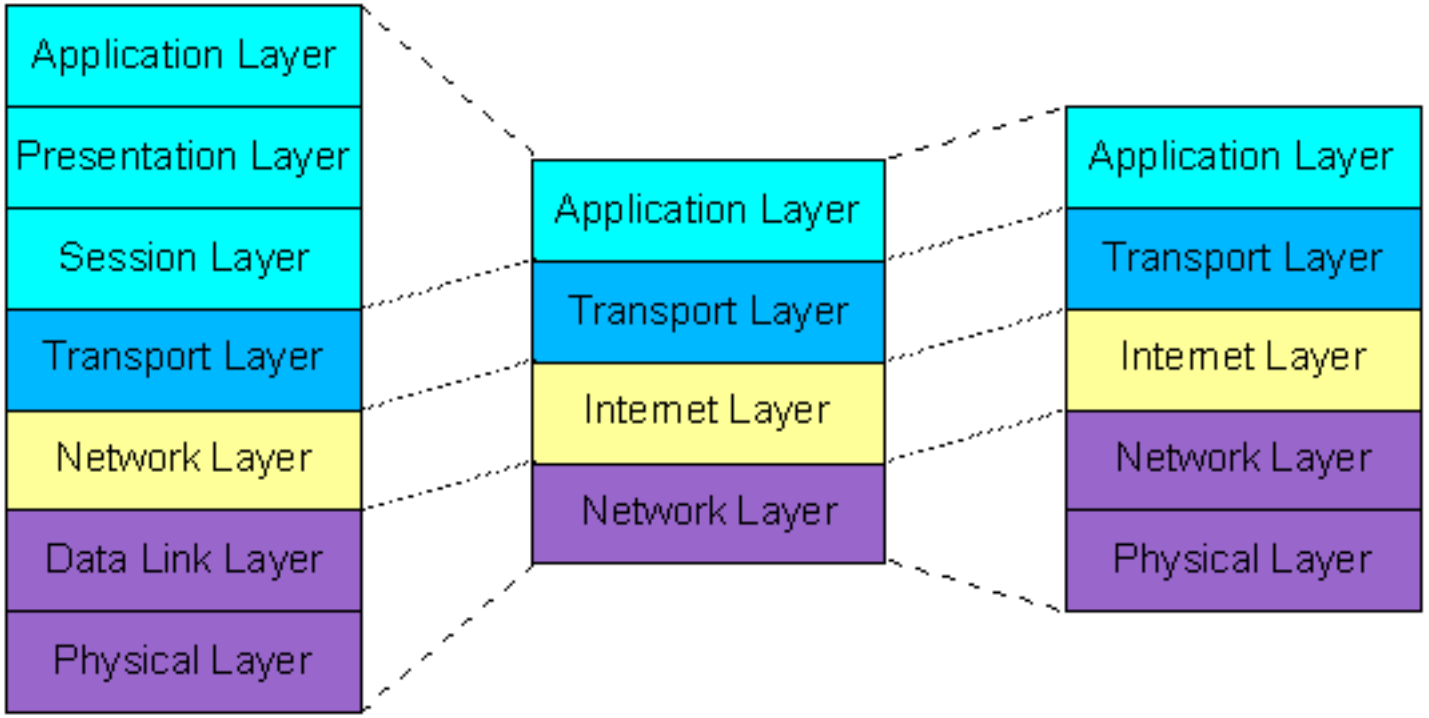
Übersicht

- Nachtrag DNS
- E-Mail:
- Internet Message Format
- MIME
- SMTP
- POP3
- Probleme mit E-Mails
- E-Mails und Privatsphäre

Erinnerung (1)

- Vorgestellt: Weg durch den Protokollstapel
- von der physikalischen Ebene (Ethernet, Token Ring, . . .)
- über logische Internetworking-Ebene (IP, . . .)
- über Transportebene (TCP, UDP, . . .)
- zur Anwendungsebene (DNS, . . .)

Erinnerung (2)



Erinnerung (3)

- Domain Name System (DNS)
- Name–Wert-Zuordnung
- verteilte Datenbank (mit verteilten Zuständigkeiten)
- hauptsächlich zur Namens*auflösung* (Name → IP-Adresse)

DNS auf dem 21C3 (1)

- *21st Chaos Communication Congress (21C3)*, Berlin 27.–29.12.2004
- Vortrag von Dan Kaminsky: Black Ops of DNS
- Wofür kann man DNS noch alles benutzen?
- z.B. Tunneln von IP
- dadurch Umgehen von z.B. Zugangsbeschränkungen möglich

DNS auf dem 21C3 (2)

- Proxy: DNS schlägt selbst nach und liefert Ergebnisse
- mehrere Ebenen von *Umleitungen (redirects)* möglich
- Ausnutzen: ein Rechner kann selbst Nameserver sein und woanders nach sich selbst fragen
- Anfrage kommt somit wieder vorbei (mit Zusatzinformationen)
- darüber z.B. Scannen des internen Netzwerks einer Firma möglich, die ihren DNS-Server sowohl von außen als auch von innen zugänglich hält

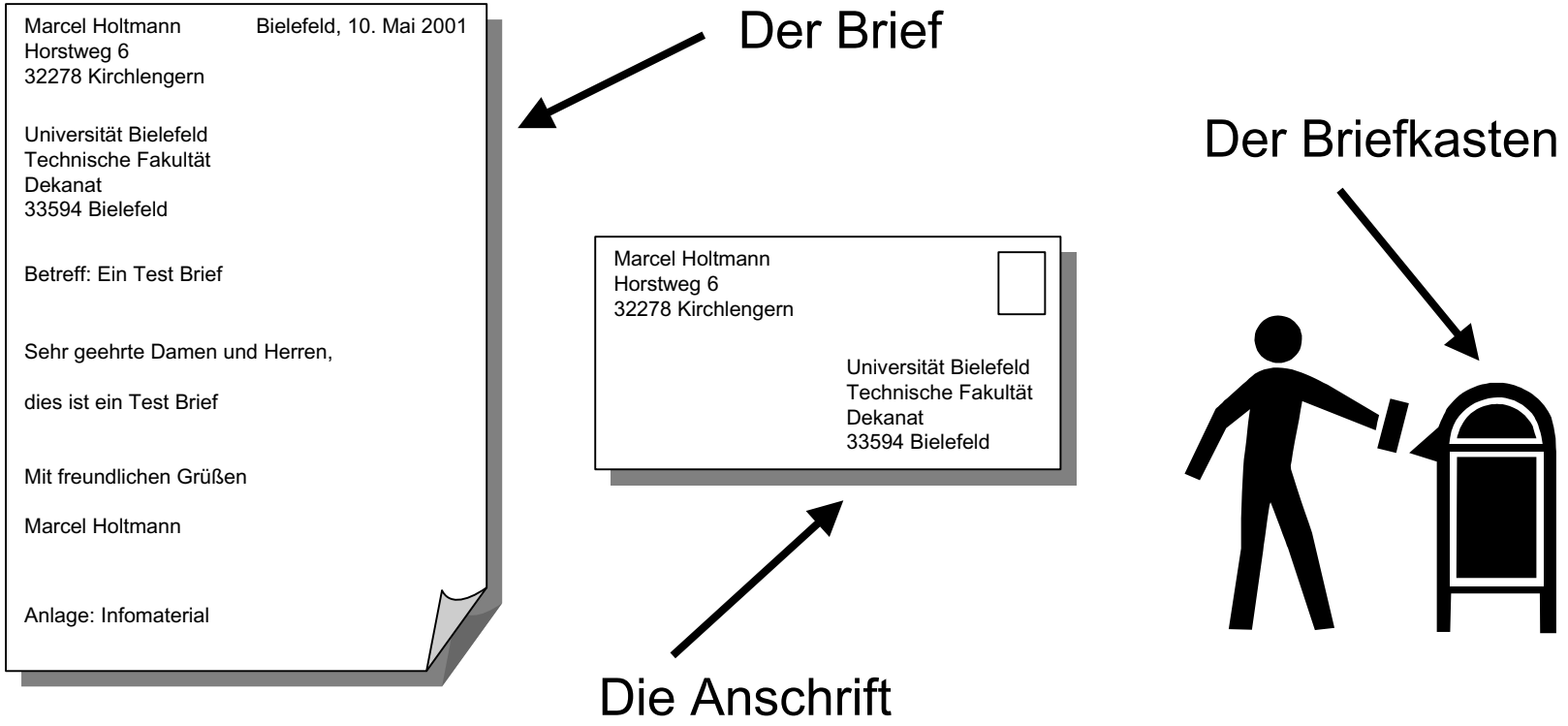
DNS auf dem 21C3 (3)

- Cache: DNS speichert erfolgreiche Anfrageergebnisse eine Weile zwischen
- Ausnutzen: Kodieren von Information in vielen Name–Wert-Zuordnungen
- Beispiel von 21C3: Distribution eines kalifornischen Radiosenders über DNS-Caching
- → DNS-Server *muß* als unsicher eingestuft werden
- Dan's Vortragsfolien: `http://www.doxpara.com/dns_tc`

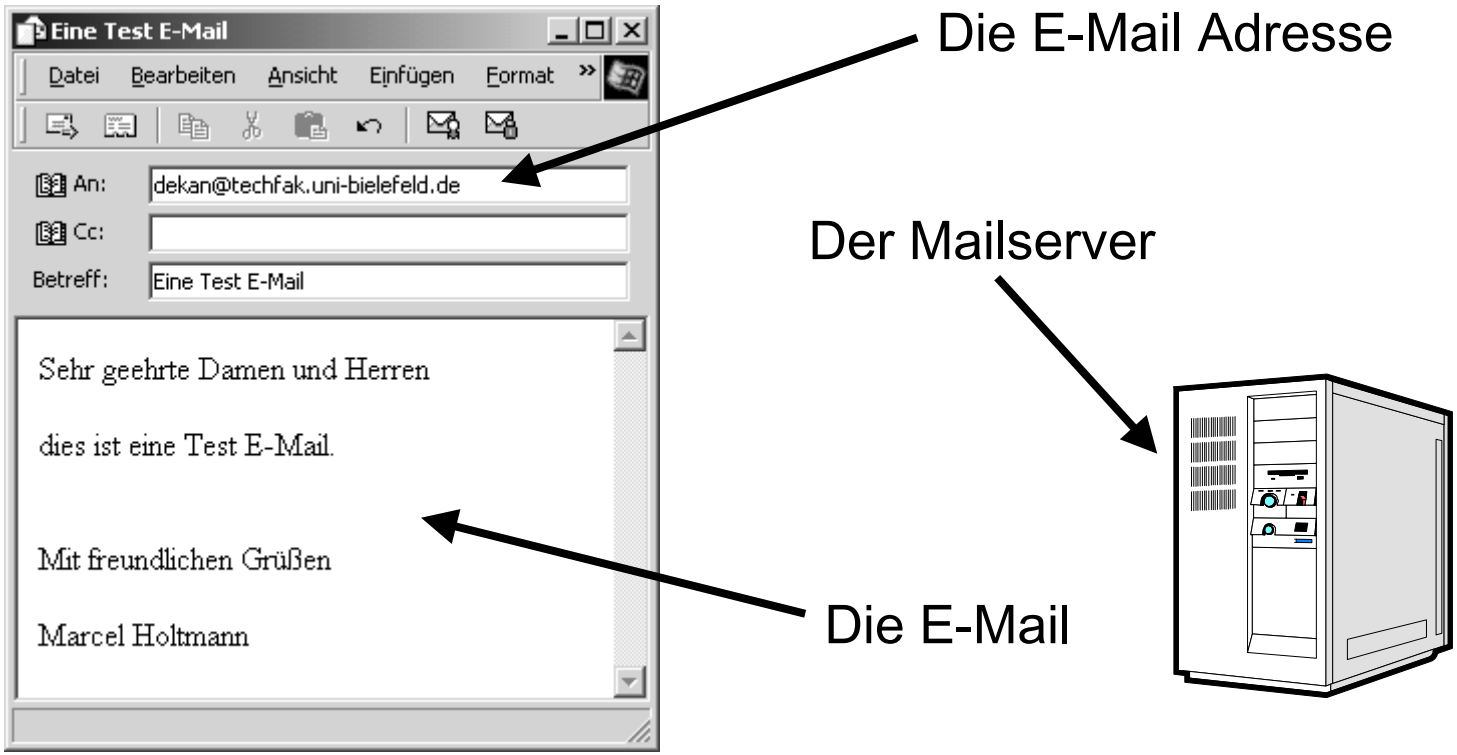
E-Mail

- eine E-Mail ist wie ein Brief oder eine Postkarte
- die E-Mail-Adresse ist wie die Anschrift
- der Briefkasten entspricht einem E-Mail-Server
- das Postamt sind die Router im Internet
- die Postautos kann man mit den Netzwerkkabeln vergleichen

Brief versenden



E-Mail versenden



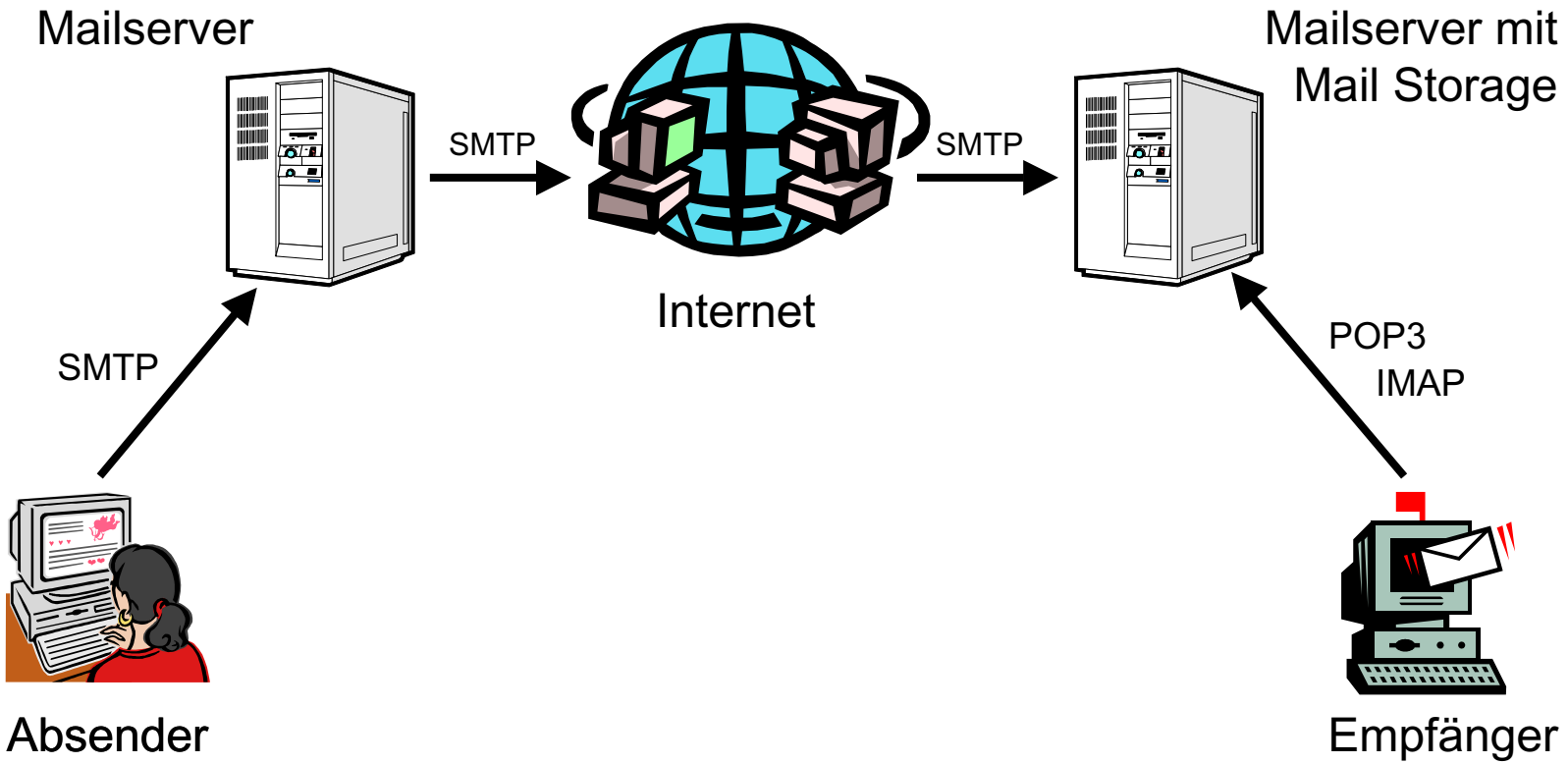
Vorteile von E-Mail

- E-Mails werden in Sekunden zugestellt –
  Die Post braucht mindestens einen Tag
- bei einem Ortswechsel kann man seine E-Mail Adresse behalten –
  Eine neue Wohnung bedeutet auch eine neue Anschrift
- eine E-Mail kann unterschiedliche Netzwerke benutzen –
  Die Deutsche Post würde nie den Dienst von z.B. UPS nutzen

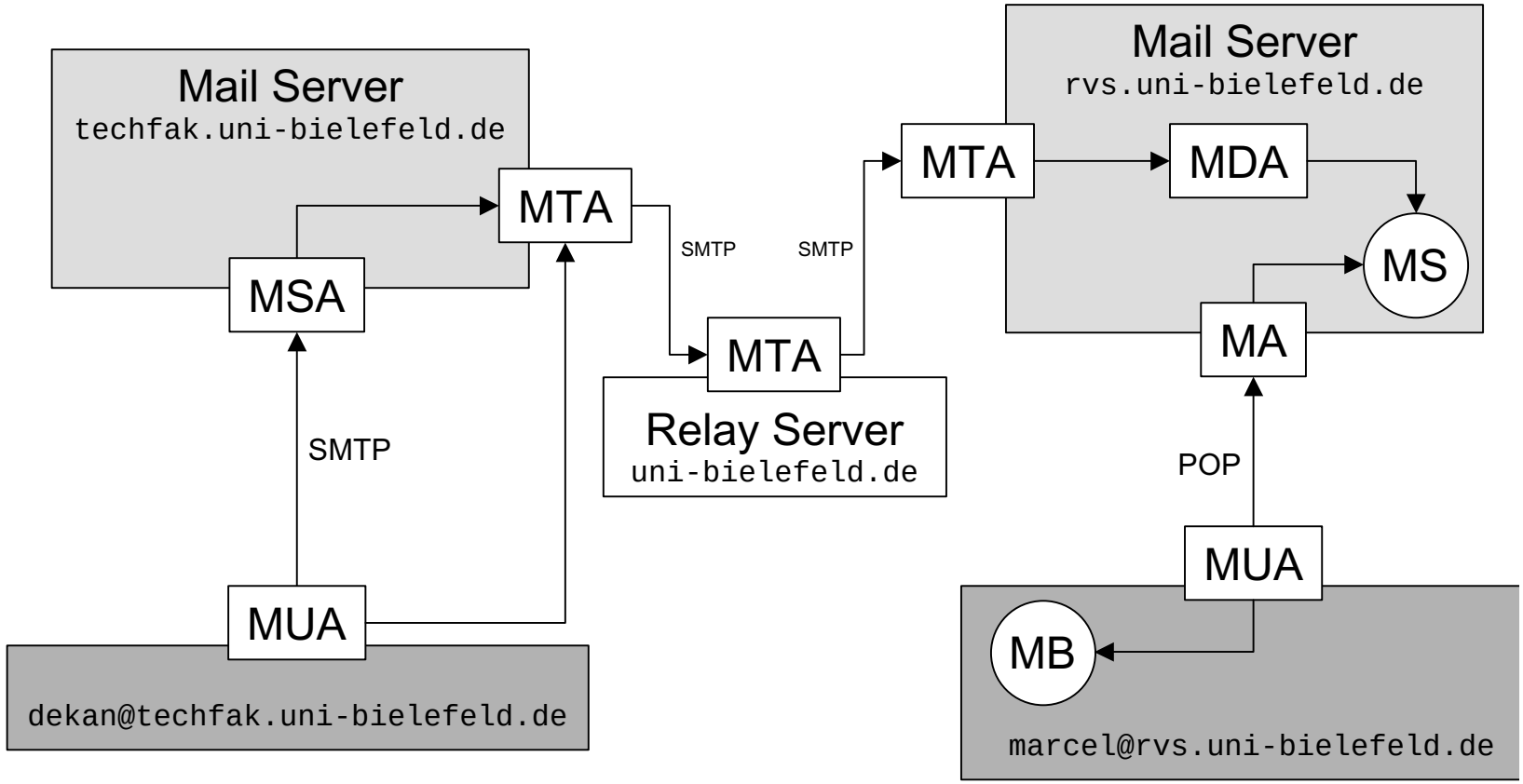
Begriffe in der E-Mail-Welt

MUA	Mail User Agent	Programm zum schreiben und lesen von E-Mails
MTA	Mail Transfer Agent	Transferiert eine Mail an einen anderen MTA
MDA	Mail Delivery Agent	Liefert eine Mail lokal aus (z.B. an MS oder MB)
MSA	Mail Submission Agent	Wartet auf eingehende Mail und übergibt sie einem MTA
MRA	Mail Retrieval Agent	Holt Mail von einem Server ab (z.B. mit POP)
MQ	Mail Queue	Warteschlange für E-Mails
MS	Mail Storage	Datenspeicher zur Aufbewahrung von E-Mails
MB	Mail Box	Lokaler Speicher von E-Mails
MF	Mail Filter	Programm oder Regeln zur Filterung von E-Mails
MA	Mail Access	Schnittstelle für den Zugriff auf MS oder MB
SMTP	Simple Mail Transfer Protocol	Protokoll zum Versenden von E-Mails
POP	Post Office Protocol	Protokoll zum Herunterladen von E-Mails

Weg einer E-Mail (1)



Weg einer E-Mail (2)



Internet Message Format

Datum	Titel	Nummer	Status
1973, Sep	Standardizing Network Mail Headers	RFC 561	Unknown
1977, Mai	Proposed standard for the format of ARPA Network messages	RFC 724	Unknown
1977, Nov	Standard for the format of ARPA network text messages	RFC 733	Unknown
1982, Aug	Standard for the format of ARPA Internet text messages	RFC 822	Historic
1988, Mär	Content-type header field for Internet messages	RFC 1049	Historic
1992, Jun	MIME (Multipurpose Internet Mail Extensions)	RFC 1341	Proposed Standard
1993, Feb	Privacy Enhancement for Internet Electronic Mail	RFC 1421	Proposed Standard
1993, Sep	MIME (Multipurpose Internet Mail Extensions)	RFC 1521	Draft Standard
1996, Okt	MIME Security with Pretty Good Privacy (PGP)	RFC 2015	Proposed Standard
1996, Nov	MIME (Multipurpose Internet Mail Extensions)	RFC 2045	Draft Standard
1998, Mär	S/MIME Version 2 Message Specification	RFC 2311	Informational
1999, Jun	S/MIME Version 3 Message Specification	RFC 2633	Proposed Standard
2001, Apr	Internet Message Format	RFC 2822	Proposed Standard

Was ist eine E-Mail-Adresse?

- lokaler Teil @ Domainname
- z.B. `jhennig@rvs.uni-bielefeld.de`
- `Jan Hennig <jhennig@rvs.uni-bielefeld.de>`
- `jhennig@rvs.uni-bielefeld.de (Jan Hennig)`

E-Mail und DNS


```
rvs.uni-bielefeld.de.   IN  SOA     matrix.rvs.uni-bielefeld.de.  hostmaster.rvs.uni-bielefeld.de. (
                                        2001053101      ; Serial
                                        3600            ; Refresh
                                        300             ; Retry
                                        604800          ; Expire (7days)
                                        172800)         ; Minimum (2days)
                        IN  NS      matrix.rvs.uni-bielefeld.de.
                        IN  MX 10   matrix.rvs.uni-bielefeld.de.
                        IN  MX 100  mail.uni-bielefeld.de.
;
mail                    IN  CNAME   matrix.rvs.uni-bielefeld.de.
matrix                  IN  A       129.70.123.10
                        IN  HINFO   "Sun Enterprise 250/2400" "SunOS 5.8"
;
project                 IN  A       129.70.123.140
                        IN  MX 10   project-mail.mit.edu.
```

```
shell >nslookup - 129.70.5.16
Standardserver: noc.hrz.uni-bielefeld.de
Address:        129.70.5.16

>set q=mx
>rvs.uni-bielefeld.de.
Server:   noc.hrz.uni-bielefeld.de
Address:  129.70.5.16

rvs.uni-bielefeld.de MX preference = 10, mail exchanger = matrix.rvs.uni-bielefeld.de
rvs.uni-bielefeld.de MX preference = 100, mail exchanger = mail.uni-bielefeld.de
matrix.rvs.uni-bielefeld.de     internet address = 129.70.123.10
mail.uni-bielefeld.de           internet address = 129.70.4.91
>
```

E-Mail im Detail

- eine E-Mail ist eine Folge von ASCII-Zeichen
- die Codierung erfolgt in 7-Bit
- deutsche Umlaute müssen anderweitig dargestellt werden
- es werden grundsätzlich drei Teile einer E-Mail unterschieden: *Header*, *Body* und *Envelope*

Grenzen einer Nachricht

- eine Zeile darf nicht mehr als 998 Zeichen enthalten (ohne <CRLF>)
- eine Zeile sollte nicht mehr als 78 Zeichen enthalten
- sowohl Header als auch Body sind nur für den Zeichensatz US-ASCII (7-Bit) definiert

Header

- ein E-Mail-Header besteht aus eine Folge von Feldern
- jedes Feld ist eine Zeile von ASCII-Zeichen
- am Anfang steht der Feldname gefolgt von einem Doppelpunkt
- ein Feldname kann jedes Zeichen außer Steuer-, dem Leerzeichen oder : enthalten
- danach kommt der Feldinhalt
- wenn ein Feldinhalt mehrere Zeilen in Anspruch nehmen soll, dann muß die neue Zeile mit mind. einem Leerzeichen beginnen

Felder im Header

Received:	Von jedem Transport Service wird eine Zeile mit Informationen über die Auslieferung hinzugefügt
From:	Die Absenderadresse
Sender:	Wenn der Sender wer anderes als der Autor der E-Mai ist
Reply-To:	Alternative Antwort Adresse
To:	Primäre Empfängeradresse
Cc:	Sekundäre Empfängeradresse (Carbon Copy)
Bcc:	Empfängeradresse die nicht angezeigt wird (Blind Carbon Copy)
Date:	Datum der E-Mail
Message-Id:	Eine weltweit eindeutige ID
Subject:	Betreffzeile eine E-Mail

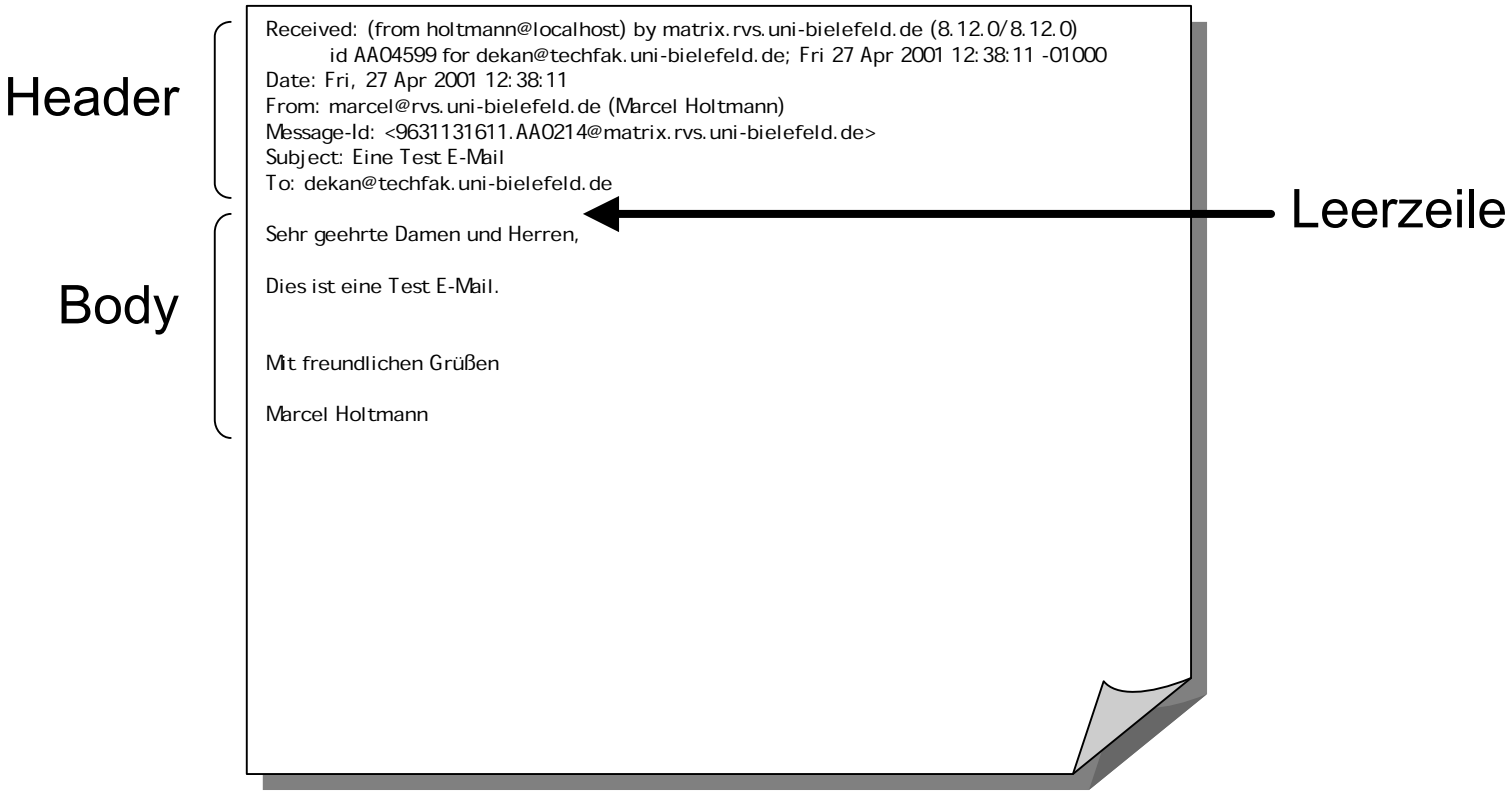
Message-ID

- eine Message-ID muss absolut eindeutig sein
- Definition dieser ID: <...@...>
- nach dem @ wird normalerweise der Hostname des versenden Servers eingetragen
- vor dem @ wird das absolute Datum mit einer Sequenznummer oder Prozess-ID benutzt
- Beispiel
  `Message-Id: <9631131611.AA0214@matrix.rvs.uni-bielefeld.de>`

Body

- nach dem Header folgt der Body einer E-Mail
- Header und Body müssen durch eine Leerzeile getrennt werden
- wenn weitere Leerzeilen folgen, gehören diese dann zur Nachricht
- im Body kann jeder 7-Bit Text enthalten sein

Beispiel


Header
Body
Leerzeile
Received: (from holtmann@localhost) by matrix.rvs.uni-bielefeld.de (8.12.0/8.12.0)
id AA04599 for dekan@techfak.uni-bielefeld.de; Fri 27 Apr 2001 12:38:11 -01000
Date: Fri, 27 Apr 2001 12:38:11
From: marcel@rvs.uni-bielefeld.de (Marcel Holtmann)
Message-Id: <9631131611.AA0214@matrix.rvs.uni-bielefeld.de>
Subject: Eine Test E-Mail
To: dekan@techfak.uni-bielefeld.de
Sehr geehrte Damen und Herren,
Dies ist eine Test E-Mail.
Mit freundlichen Grüßen
Marcel Holtmann

Envelope

- der Envelope spielt bei dem Format einer Internet Message selbst noch keine Rolle
- beim Übertragen einer Nachricht aber wird der Envelope angegeben und benutzt
- die Daten vom Envelope sind normalerweise auch im Header einer E-Mail enthalten
- Transportmitteilungen werden jeweils *vorne* angefügt
- dies muß jedoch nicht zwangsläufig bei jedem Transportmedium so sein

Multipurpose Internet Mail Extensions

Datum	Titel	Nummer	Status
1988, Mär	Content-type header field for Internet messages	RFC 1049	Historic
1992, Jun	MIME (Multipurpose Internet Mail Extensions)	RFC 1341	Proposed Standard
1993, Feb	Privacy Enhancement for Internet Electronic Mail	RFC 1421	Proposed Standard
1993, Sep	MIME (Multipurpose Internet Mail Extensions)	RFC 1521	Draft Standard
1996, Okt	MIME Security with Pretty Good Privacy (PGP)	RFC 2015	Proposed Standard
1996, Nov	MIME (Multipurpose Internet Mail Extensions)	RFC 2045	Draft Standard
1998, Mär	S/MIME Version 2 Message Specification	RFC 2311	Informational
1999, Jun	S/MIME Version 3 Message Specification	RFC 2633	Proposed Standard
2001, Apr	Internet Message Format	RFC 2822	Proposed Standard

Probleme von RFC 822

- RFC 822 definiert nur Textnachrichten
- es ist nur für 7-Bit US-ASCII definiert
- eine Zeile kann nur 1000 Zeichen lang sein
- es gibt keine Möglichkeit Multimediadaten zu übertragen, wie z.B. Bilder

Ideen von MIME

- Texte in anderen Formaten wie US-ASCII
- andere Formate für den Message Body, wie z.B. Bilder oder Office-Dokumente
- mehrere unterschiedliche Formate in einer Mail
- alternative Inhalte in einer Nachricht, wie z.B. zwei verschiedene Sprachversionen
- nicht-US-ASCII-Informationen in den Feldern des Header, z.B. Umlaute im Subject

MIME ist eine Reihe von RFCs

- RFC 2045: Part I Format of Internet Message Bodies
- RFC 2046: Part II Media Types
- RFC 2047: Part III Message Header Extensions for Non-ASCII Text
- RFC 2048: Part IV Registration Procedures
- RFC 2049: Part V Conformance Criteria and Examples

Definition von MIME

- Part I definiert das allgemeine Format:
- MIME-Version header field
- Content-Type header field
- Content-Transfer-Encoding header field
- Content-ID header field
- Content-Description header field

MIME-Version Header Field

- jede Nachricht, die MIME benutzt, muß dieses Feld enthalten
- bis jetzt gibt es MIME nur in der Version 1.0
- für Dokumente mit anderen Versionsnummern gilt diese Definition nicht
- Beispiele:

```
MIME-Version: 1.0
MIME-Version: 1.0 (produced by MetaSend Vx.x)
```

Content-Type Header Field

- zuerst definiert in RFC 1049
- ein *Content-Type* besteht aus einem Typ, einem Subtyp und weiteren Parametern
- RFC-822-Nachrichten ohne Header sind: `Content-type: text/plain; charset=us-ascii`
- mögliche Typen sind: `text`, `image`, `audio`, `video`, `application`, `message`, `multipart`
- weitere Typen werden mit einem `x-` gekennzeichnet
- Subtypen werden von der IANA definiert

Content-Id und Content-Description

- Content-ID ist analog zur Message-ID und muß weltweit eindeutig sein
- Content-Description enthält eine einfache Beschreibung des Inhalts (z.B. „Bild von meinem Haus in Spanien“)
- für die Zukunft sind alle Felder, die mit `Content-` anfangen für MIME reserviert

Content-Transfer-Encoding

- definiert das Format für den Body
- mögliche Werte sind: `7bit` , `8bit` , `binary` , `quoted-printable` , `base64`, `ietf-token`, `x-token`
- nicht alle Werte können mit SMTP als Transportmedium benutzt werden
- Standardwert ist hier `7bit`

Quoted-Printable und BASE64

- MIME definiert *BASE64* und *Quoted-Printable*
- Quoted-Printable dient zur Maskierung von Sonderzeichen oder Umlauten
- BASE64 ist zum Transport von binären Daten gedacht (wie z.B. Bilder)
- beide Verfahren liefern eine Folge von Textzeichen in US-ASCII (7-Bit)

Eigenschaften von BASE64

- BASE64 verwandelt 8-Bit Daten in 6-Bit Text
- es werden nur die Zeichen A-Z, a-z, +, /, 0-9 und = benutzt
- Eine Datei in BASE64 ist 33% größer als die ursprüngliche Datei
- die Programme uuencode und uudecode leisten diese Arbeit unter Unix/Linux

MIME Message

- es gibt zwei Arten von *Multipart*:
  - mixed
  - alternative
- es gibt mehrere Varianten von *Message*:
  - rfc822
  - partial
  - external-body

MIME Beispiel


```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Date: Sun, 21 Mar 1993 23:56:48 -0800 (PST)
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary="simple boundary"

This is the preamble.  It is to be ignored, though it
is a handy place for composition agents to include an
explanatory note to non-MIME conformant readers.

--simple boundary

This is implicitly typed plain US-ASCII text.
It does NOT end with a linebreak.
--simple boundary
Content-type: text/plain; charset=us-ascii

This is explicitly typed plain US-ASCII text.
It DOES end with a linebreak.

--simple boundary--

This is the epilogue.  It is also to be ignored.
```

```
From: Bill@host.com
To: joe@otherhost.com
Date: Fri, 26 Mar 1993 12:59:38 -0500 (EST)
Subject: Audio mail (part 1 of 2)
Message-ID: <id1@host.com>
MIME-Version: 1.0
Content-type: message/partial; id="ABC@host.com"; number=1; total=2

Message-ID: <anotherid@foo.com>
Subject: Audio mail
MIME-Version: 1.0
Content-type: audio/basic
Content-transfer-encoding: base64

... first half of encoded audio data goes here ...
```

```
From: Bill@host.com
To: joe@otherhost.com
Date: Fri, 26 Mar 1993 12:59:38 -0500 (EST)
Subject: Audio mail (part 2 of 2)
MIME-Version: 1.0
Message-ID: <id2@host.com>
Content-type: message/partial; id="ABC@host.com"; number=2; total=2

... second half of encoded audio data goes here ...
```

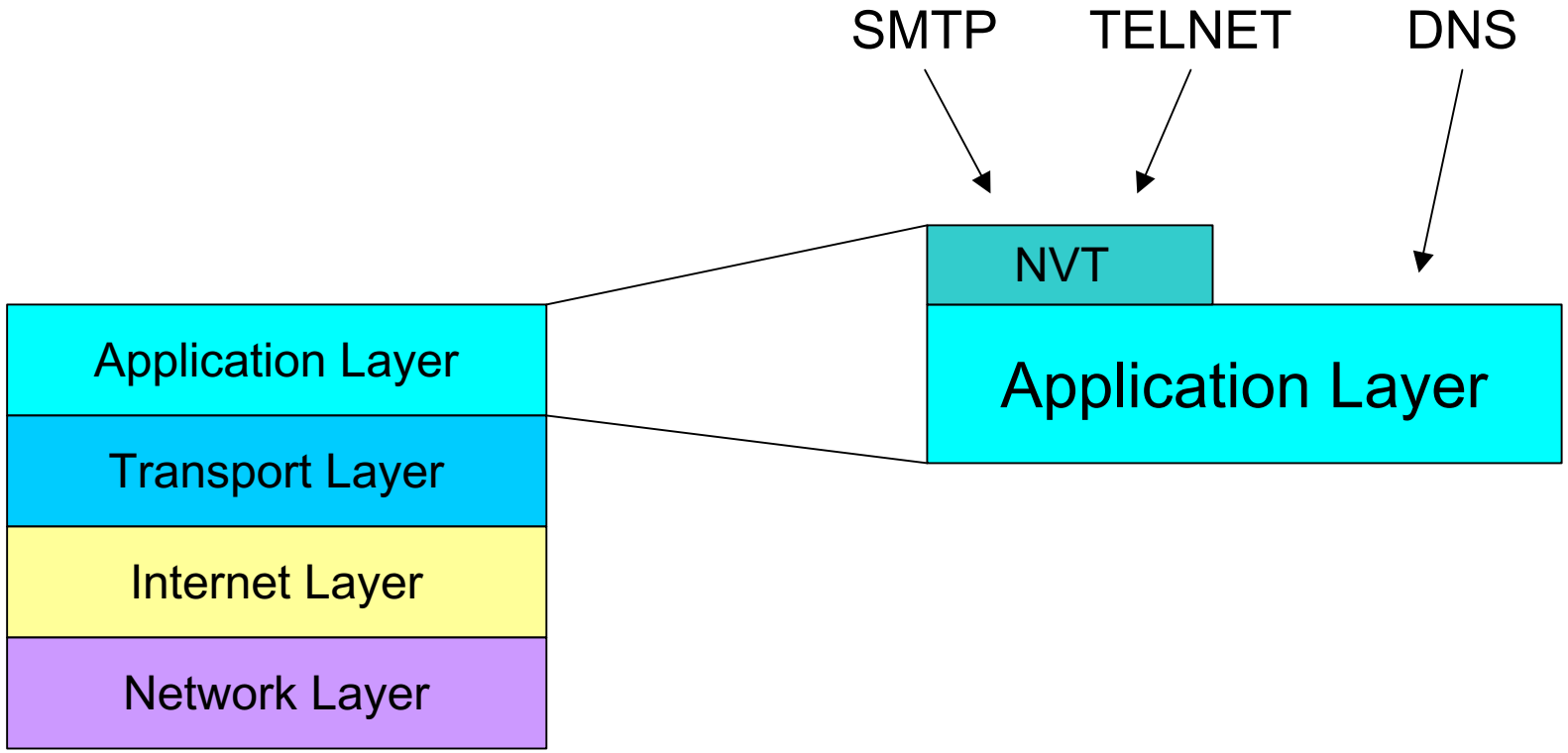
Ports für E-Mail


```
smtp        25/tcp    mail          # Simple Mail Transfer Protocol

pop2        109/tcp                 # Post Office Protocol - Version 2
pop3        110/tcp                 # Post Office Protocol - Version 3

imap        143/tcp   imap2 imap4   # Internet Message Access Protocol
imap3       220/tcp                 # Interactive Mail Access Protocol v3

imsp        406/tcp                 # Internet Message Support Protocol
acap        674/tcp                 # Application Configuration Access Protocol

smtps       465/tcp                 # SMTP protocol over TLS/SSL (deprecated)
imap4-ssl   585/tcp                 # IMAP4 + SSL (use 993 instead)
imaps       993/tcp                 # IMAP protocol over TLS/SSL
pop3s       995/tcp                 # POP3 protocol over TLS/SSL
```

Network Virtual Terminal

- RFC 854 – Telnet Protocol Specification
- fiktive Ein-/Ausgabe-Einheit mit bekannten Eigenschaften
- zeilenorientiert und Bidirektional
- (per default) 7-Bit-ASCII in 8-Bit-Wort
- unbegrenzte Zeilen- und Seitenlänge
- Steuerfunktionen

NVT im Schichtenmodell



Simple Mail Transport Protocol (1)

Datum	Titel	Nummer	Status
1973, Feb	Mail retrieval via FTP	RFC 458	Unknown
1973, Mär	FTP and network mail system	RFC 475	Unknown
1973, Jun	Proposed Mail Protocol	RFC 524	Unknown
1973, Jul	Thoughts on the mail protocol proposed in RFC 524	RFC 539	Unknown
1978, Dez	Survey of FTP mail and MLFL	RFC 751	Unknown
1980, Sep	Mail Transfer Protocol	RFC 772	Unknown
1981, Mai	Mail Transfer Protocol	RFC 780	Unknown
1981, Nov	Simple Mail Transfer Protocol	RFC 788	Unknown
1982, Aug	Simple Mail Transfer Protocol	RFC 821	Historic
1986, Feb	UUCP mail interchange format standard	RFC 976	Unknown
1993, Feb	SMTP Service Extensions	RFC 1425	Proposed Standard
1993, Feb	SMTP Service Extension for 8bit-MIMEtransport	RFC 1426	Proposed Standard
1993, Feb	SMTP Service Extension for Message Size Declaration	RFC 1427	Proposed Standard

Simple Mail Transport Protocol (2)

Datum	Titel	Nummer	Status
1994, Jul	SMTP Service Extensions	RFC 1651	Draft Standard
1994, Jul	SMTP Service Extension for 8bit-MIMEtransport	RFC 1652	Draft Standard
1994, Jul	SMTP Service Extension for Message Size Declaration	RFC 1653	Draft Standard
1995, Aug	SMTP Service Extensions for Large and Binary Messages	RFC 1830	Experimental
1995, Nov	SMTP Service Extensions	RFC 1869	Standard
1995, Nov	SMTP Service Extension for Message Size Declaration	RFC 1870	Standard
1996, Jan	SMTP Service Extension for Delivery Status Notifications	RFC 1891	Proposed Standard
1996, Jan	Enhanced Mail System Status Codes	RFC 1893	Proposed Standard
1996, Aug	SMTP Service Extension for Remote Message Queue Starting	RFC 1985	Proposed Standard
1996, Okt	Local Mail Transfer Protocol	RFC 2033	Informational
1996, Okt	SMTP Service Extension for Returning Enhanced Error Codes	RFC 2034	Proposed Standard
1998, Dez	Message Submission	RFC 2476	Proposed Standard
1999, Jan	SMTP Service Extension for Secure SMTP over TLS	RFC 2487	Proposed Standard

Simple Mail Transport Protocol (3)

Datum	Titel	Nummer	Status
1999, Feb	Anti-Spam Recommendations for SMTP MTAs	RFC 2505	Best Current Practic
1999, Mär	SMTP Service Extension for Authentication	RFC 2554	Proposed Standard
1999, Aug	ON-DEMAND MAIL RELAY SMTP with Dynamic IP Addresses	RFC 2645	Proposed Standard
2000, Jun	Deliver By SMTP Service Extension	RFC 2852	Proposed Standard
2000, Dez	SMTP Service Extensions for Large and Binary Messages	RFC 3030	Proposed Standard
2001, Apr	Simple Mail Transfer Protocol	RFC 2821	Proposed Standard

E-Mail mit SMTP

- benutzt gesicherten Transport Service von TCP
- NVT-Dienst an TCP-Port 25
- maximal 1000 Zeichen pro Zeile erlaubt
- TCP/IP und SMTP machen die E-Mail-Kommunikation universell
- MIL-Standard 1781

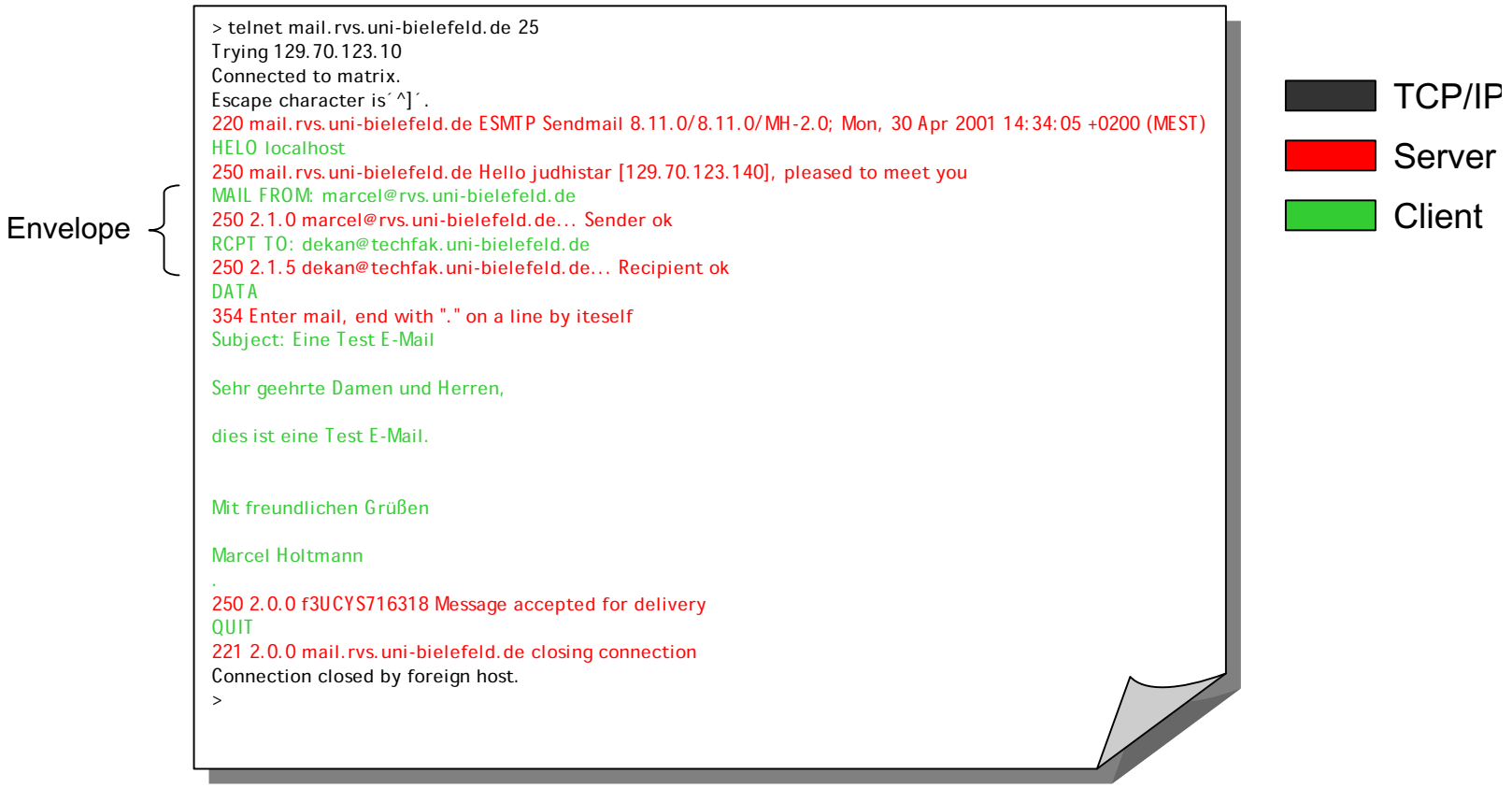
Minimale SMTP Kommandos

HELO <hostname>	Begrüßung des SMTP-Servers
MAIL FROM: <addr>	Absenderadresse
RCPT TO: <addr>	Empfängeradresse
DATA	Den Text der E-Mail nach RFC 822 (mit Header) gefolgt von einem abschließenden „<CRLF>.<CRLF>“
RSET	Zurücksetzen einer Verbindung
NOOP	No Operation
QUIT	Verbindung beenden

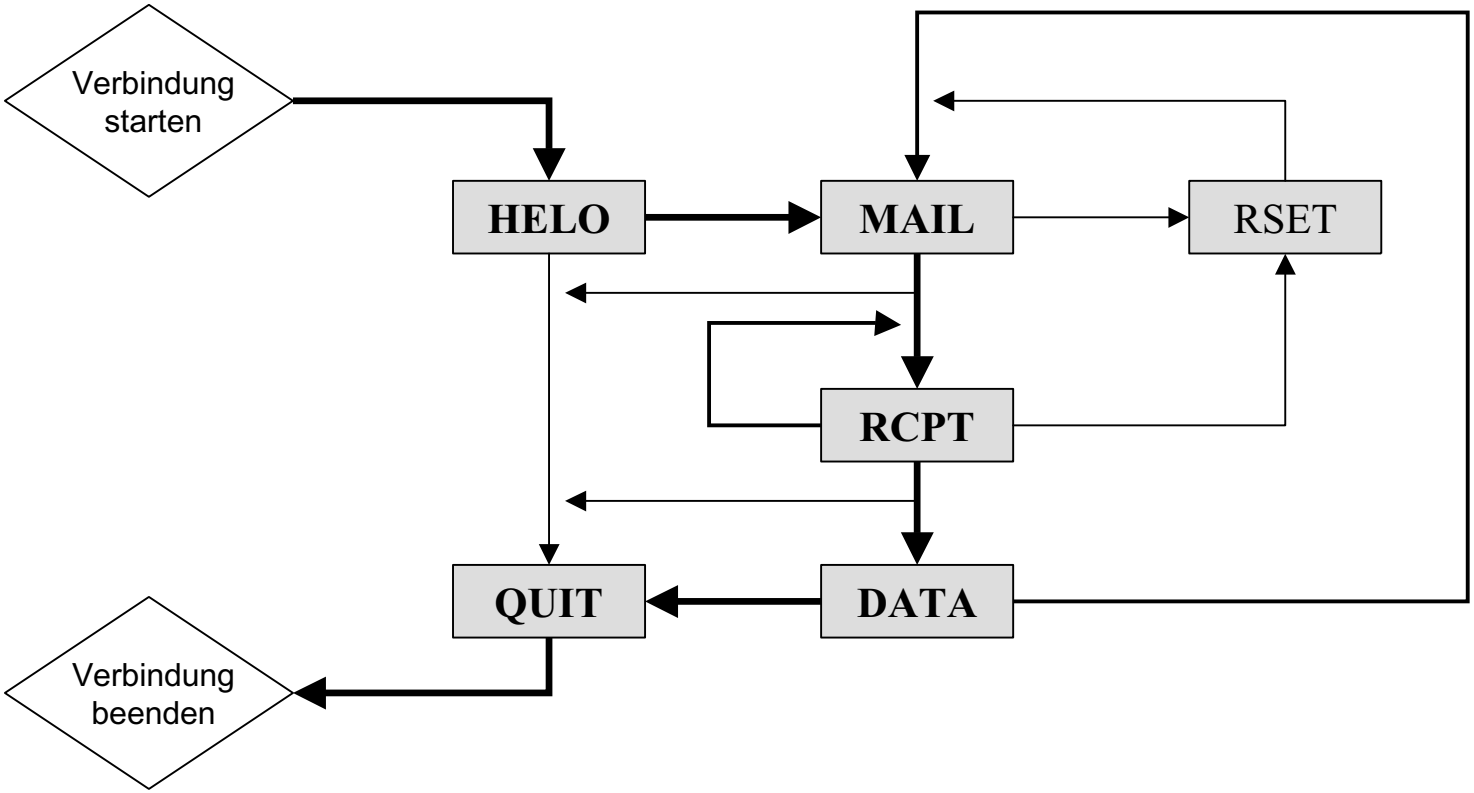
Zusätzliche SMTP Kommandos

VRFY <addr>	Kontrollieren einer E-Mail Adresse
EXPN <addr>	Auflösen einer Mailing List
SEND FROM: <addr>	E-Mail and Terminal senden
SOML FROM: <addr>	Send or Mail
SAML FROM: <addr>	Send and Mail
TURN	Vertauschen der Rollen zwischen Client und Server
HELP <string>	Hilfe zu Befehlen

Eine SMTP-Sitzung

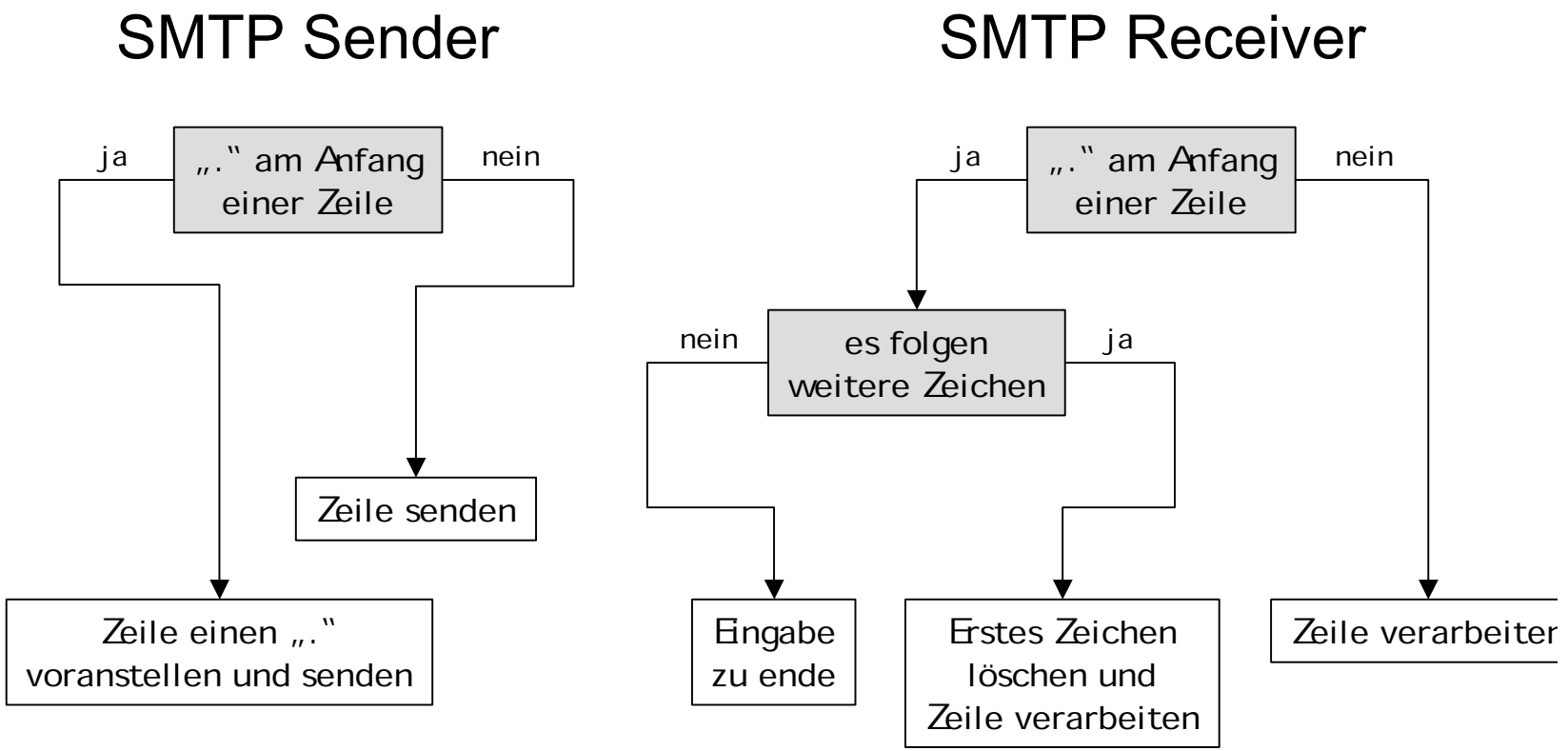


Reihenfolge der Kommandos



Das Problem mit dem Punkt

- die Zeichenfolge <CRLF>.<CRLF> kennzeichnet das Nachrichtenende und kann ohne weiteres nicht gesendet werden
- z.B.: die Nachricht hat eine Zeile, welche nur aus einem Punkt besteht
- oder: eine Zeile hat einen Punkt am Anfang, gefolgt von mehreren Zeichen
- was ist eine gute und einfache Lösung?


SMTP Sender
ja
„.“ am Anfang einer Zeile
nein
Zeile senden
Zeile einen „.“ voranstellen und senden
SMTP Receiver
ja
„.“ am Anfang einer Zeile
nein
nein
es folgen weitere Zeichen
ja
Eingabe zu ende
Erstes Zeichen löschen und Zeile verarbeiten
Zeile verarbeiten

SMTP-Reply-Codes

- ein Reply besteht aus einer 3-stelligen Zahl
- gefolgt von einem Leerzeichen oder –
- zusätzlich gibt es noch einen Text-String
- Erweiterung im Text-String: Hinter dem Standard Statuscode wird ein weiterer Code angegeben
- class.subject.detail
  z.B. `550 5.1.1 Mailbox “dekan“ does not exist`
- weiterhin kompatibel zu allen Clients

Erste Ziffer im Reply-Code

1yz	**Positive Preliminary reply** Positiver Beginn eines Befehls. Weitere Eingabe erforderlich.
2yz	**Positive Completion reply** Positive Beendigung eines Befehls. Es können weitere Befehle gesendet werden.
3yz	**Positive Intermediate reply** Positiver Zwischenzustand. Weitere Eingaben müssen folgen.
4yz	**Transient Negative Completion reply** Transientes Problem. Befehl wurde nicht ausgeführt. Eingabe wiederholen.
5yz	**Permanent Negative Completion reply** Definitives Problem. Befehl nicht wiederholen.

Zweite und dritte Ziffer

x0z	**Syntax eines Befehls**
x1z	**Allgemeine Information**
x2z	**Verbindungszustand**
x3z	**Nicht spezifiziert**
x4z	**Nicht spezifiziert**
x5z	**Statusmeldung**

xyz	**z = Weitere Unterteilung/Nummerierung der Meldung**

Liste der Reply-Codes

500 Syntax error, command unrecognized
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented

211 System status, or system help reply
214 Help message

220 <domain> Service ready
221 <domain> Service closing
transmission channel
421 <domain> Service not available,
closing transmission channel

250 Requested mail action okay, completed
251 User not local; will forward to <forward-path>
450 Requested mail action not taken: mailbox unavailable
550 Requested action not taken: mailbox unavailable
451 Requested action aborted: error in processing
551 User not local; please try <forward-path>
452 Requested action not taken: insufficient system storage
552 Requested mail action aborted: exceeded storage allocat
553 Requested action not taken: mailbox name not allowed
354 Start mail input; end with <CRLF>.<CRLF>
554 Transaction failed

Erweiterung von SMTP

- die SMTP-Service-Extensions werden im allgemeinen als ESMTP bezeichnet
- `EHLO` wird als alternative und erweiternde Begrüßung eingeführt
- die Befehle `MAIL FROM:` und `RCPT TO:` können zusätzliche Parameter bekommen
- mit dem RFC 2821 wurden SMTP und ESMTP zu einem Standard zusammengefügt

SMTP und Relaying

- man kann jede beliebige Absenderadresse beim SMTP-Protokoll angeben
- hierdurch kann man vorgeben jemand zu sein, der man gar nicht ist
- ein anderer Server kann vorübergehend Mails aufnehmen und zwischenspeichern
- Grundprinzip: Jeder hilft jedem.

Das Problem mit SPAM

- mit SMTP ist es einfach eine E-Mail an ganz viele Empfänger auf einmal zu schicken
- für den Absender ist es nur eine Nachricht
- der SMTP Server hingegen muss jede E-Mail einzeln ausliefern
- Ausnutzung zum einfachen und schnellen Massenversand von Werbung

Vermeidung von SPAM

- der Server nimmt nur Nachrichten an, die als Empfänger einen Benutzer des Systems haben
- nur festgelegte IP-Adressen dürfen E-Mails an andere verschicken
- bekannte Adressen von Spammern werden blockiert (z.B. durch Blacklists)
- ein Benutzer muss sich beim SMTP Server anmelden um E-Mails zu verschicken
- es gibt entsprechende SMTP-Erweiterungen mit Authentifizierung, jedoch wenig verbreitet

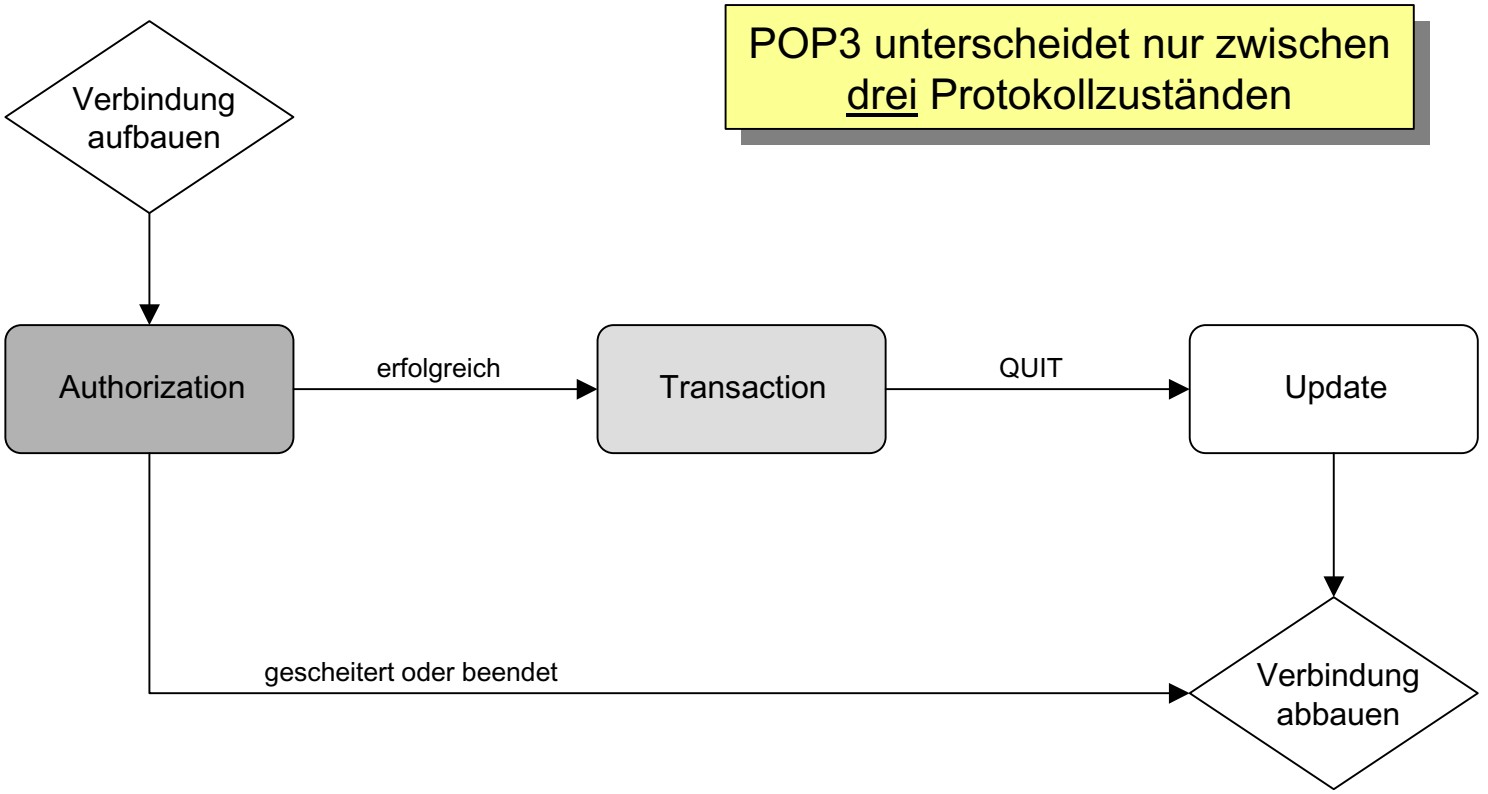
Abholen von Mail: POP

- *Post Office Protocol Version 3 (POP3)*
- Protokoll für den Zugriff auf ein Postfach
- *download-and-delete*-Modell
- ASCII-basiertes Protokoll
- einfach zu implementieren durch NVT
- weit verbreitet und in jedem Client vorhanden
- aktueller Standard im RFC 1939 von Mai 1996

Entstehung von POP3

Datum	Titel	Nummer	Status
1984, Okt	Post Office Protocol	RFC 918	Unknown
1985, Feb	Post Office Protocol: Version 2	RFC 937	Historic
1988, Nov	Post Office Protocol: Version 3	RFC 1081	Unknown
1991, Mai	Post Office Protocol: Version 3	RFC 1225	Draft Standard
1993, Jun	Post Office Protocol: Version 3	RFC 1460	Draft Standard
1994, Nov	Post Office Protocol: Version 3	RFC 1725	Standard
1994, Dez	POP3 AUTHentication command	RFC 1734	Proposed Standar
1996, Mai	Post Office Protocol: Version 3	RFC 1939	Standard
1997, Jan	IMAP/POP AUTHorize Extension for Simple Challenge/Response	RFC 2095	Proposed Standar
1997, Sep	IMAP/POP AUTHorize Extension for Simple Challenge/Response	RFC 2195	Proposed Standar
1998, Nov	POP3 Extension Mechanism	RFC 2449	Proposed Standar
1999, Jun	Using TLS with IMAP, POP3 and ACAP	RFC 2595	Proposed Standar

POP ist einfach



POP3-Kommandos Authorisierung

Minimale POP3 Kommandos

USER name	Übergabe eines Mailboxnamen
PASS string	Eingabe eines Passwortes
QUIT	Beenden der POP3 Session

Optionale POP3 Kommandos

APOP name digest	Alternative Autorisierung mit Hilfe eines Digest. Dient zur Vermeidung von Klartextpasswörtern.

POP3-Kommandos Transaktion

Minimale POP3 Kommandos

STAT	Nachrichtenanzahl und Größe
LIST [msg]	Liste der Nachrichten
RETR msg	Nachricht abfragen
DELE msg	Nachricht löschen
NOOP	No operation
RSET	Reset
QUIT	Session beenden

Optionale POP3 Kommandos

TOP msg n	Nur Header und die ersten n Zeilen abfragen
UIDL [msg]	Einheitliche ID für Nachrichten abfragen

POP3-Antworten

- eine Antwort kann 512 Zeichen lang sein (inklusive dem abschließenden CRLF)
- sie besteht aus einem Statusindikator und einer Nachricht in Klartext
- es gibt positive (+OK) und negative (-ERR)
- +OK und -ERR müssen in Großbuchstaben gesendet werden
- manche Antworten enthalten weitere Informationen, wie z.B. die Zahl der Nachrichten oder dessen Größe

Multi-Line-Antworten

- es gibt Kommandos die mehrere Zeilen Antwort an den Client zurückliefern
- ob ein Kommando mehrere Antwortzeilen enthält ist klar und eindeutig im RFC definiert
- jede Multi-Line-Antwort beginnt in der ersten Zeile genauso wie alle Antworten
- das Ende wird durch CRLF.CRLF signalisiert
- für die Codierung des Punkts am Anfang einer Zeile gelten die gleichen Regeln wie bei SMTP

POP3-Beispiel

Authorization

Transaction

```
> telnet mail.rvs.uni-bielefeld.de 110
Trying 129.70.123.10
Connected to matrix.
Escape character is´^]´.
+OK QPOP (version 2.53) at matrix starting.  <27476.928927903@matrix>
user holtmann
+OK Password required for holtmann.
pass sagichnicht
+OK holtmann has 1 message (423 octets).
stat
+OK 1 423
retr 1
+OK 423 octets
Received: (from holtmann@localhost)
        by mail.rvs.uni-bielefeld.de (8.9.2/8.9.1) id NAA27468
        for holtmann; Wed, 9 Jun 1999 13:31:29 +0200 (MET DST)
Date: Wed, 9 Jun 1999 13:31:29 +0200 (MET DST)
From: Marcel Holtmann <marcel@rvs.uni-bielefeld.de>
Message-Id: <199906091131.NAA27468@mail.rvs.uni-bielefeld.de>
Content-Type: text
X-UIDL: 24766cbf641bf2ad3c050a0ea15a9069

Hallo dies ist eine Test-Mail

.
dele 1
+OK Message 1 has been deleted.
quit
+OK Pop server at matrix signing off.
Connection closed by foreign host.
>
```

TCP/IP
Server
Client

Die AUTH-Erweiterung (1)

- RFC 1734 definiert den Befehl AUTH
- generische Methode zur Authentifizierung
- ohne Parameter listet der Befehl alle unterstützten Authentifizierungsverfahren auf
- als Parameter muß ein Verfahren angegeben werden

Die AUTH-Erweiterung (2)

- der Server antwortet mit einem + gefolgt von einem Leerzeichen und einer Zeichenkette in BASE64
- der Client schickt die Antwort auch in BASE64
- eine Authentisierung kann mehrstufig sein
- wird ein * vom Client gesendet, so wird ein Abbruch der Anmeldung eingleitet
- antwortet der Server mit -ERR ist die Anmeldung fehlgeschlagen oder es wurde abgebrochen
- bei +OK wechselt der Server erfolgreich in den Transaction-Zustand

AUTH-Beispiel


```
+OK POP3 server ready
auth
PLAIN
CRAM-MD5
KERBEROS_V4
.
auth KERBEROS_V4
+ AmFYig==
BAcAQU5EUkVXLkNNVS5FRFUAOCAsho84kLN3/IJmrMG+25a4DT+nZImJjnTNHJUtxAA+oOKPKfHE
cAFs9a3CL5Oebe/ydHJUwYFdWwuQ1MWiy6lesKvjL5rL9WjXUb9MwT9bpObYLGOKi1Qh
+ or//EoAADZI=
DiAF5A4gA+oOIALuBkAAmw==
+OK Kerberos V4 authentication successful



auth foobar
-ERR Unrecognized authentication type
```

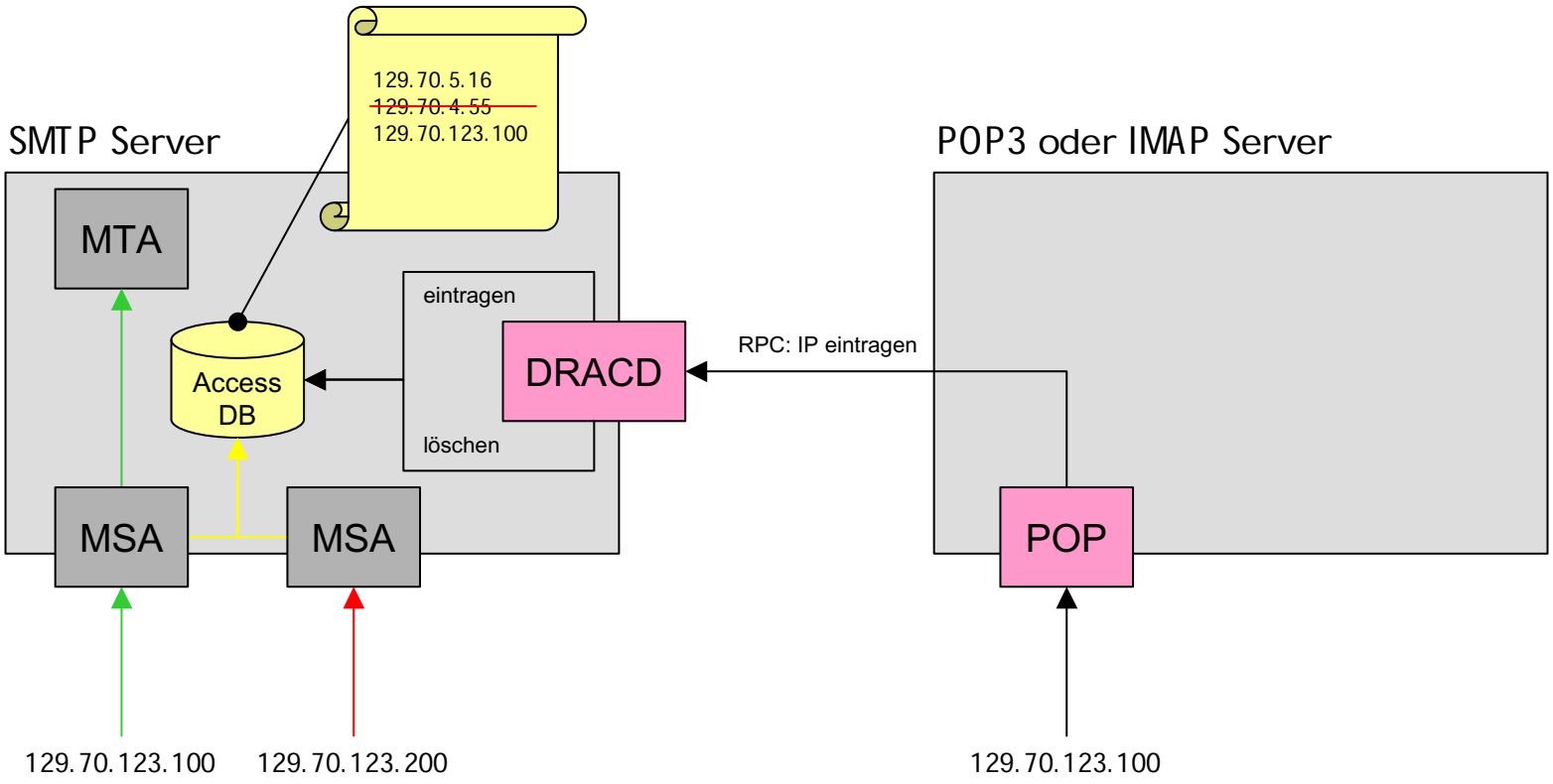
Server

Client

SMTP after POP

- das POP-Protokoll unterstützt eine Authentisierung – SMTP aber nicht
- Dynamic Relay Authorization Control (DRAC)
  `http://mail.cc.umanitoba.ca/drac/`
- ein Benutzer holt seine E-Mails mit POP3 ab
- er muss sich beim Server anmelden
- danach wird dem SMTP-Server die IP-Adresse der Anfrage mitgeteilt
- der SMTP-Server erlaubt ein Relaying von dieser IP-Adresse für eine bestimmte Zeit
- nun kann der Benutzer mit SMTP Mails versenden

DRAC-Funktionsweise



Sicherheit bei Internet Messages

- Verschlüsselung des Inhalts einer E-Mail: S/MIME oder PGP
- Verschlüsselung der Kommunikation über die Protokolle SMTP und POP3 mit einem verschlüsselten Tunnel
- Verschlüsselung des Login-Mechanismus (AUTH, CRAM-MD5, . . .)

Welche Sicherheit ist sinnvoll?

- die Verschlüsselung des Kennwortes
- bei geheimen Inhalten sollte immer S/MIME oder PGP benutzt werden
- was aber sind geheime Inhalte?
- Vertrauliches? Geschäfts-Korrespondenzen? Alles?

Aktuelle Spiegel-Meldung

SPIEGEL ONLINE NETZWELT

Ressort wählen | Image | Übersicht | Netzpolitik | Technologie | Netzkultur

Home > Netzwelt > Netzpolitik

22. Dezember 2004 Druckversion | Versenden | Leserbrief

DIGITALER LAUSCHANGRIFF

Ab Januar gehen verdächtige E-Mails CC an die Polizei

Eine neue Verordnung erlaubt es dem Staat, den E-Mail-Verkehr besser zu überwachen. Ab dem 1. Januar 2005 haben Kommunikationsanbieter die für staatliches Lauschen erforderliche Technik einzurichten - auf eigene Kosten. Datenschützer und die betroffene Provider sind empört.

DPA

Lauschangriff: Die Abhörmöglichkeiten wurden in den letzten zehn Jahren kontinuierlich erweitert

"Es rechnet sich nicht mehr", klagt Frank Simon, Geschäftsführer des Providers ECCE TERRAM im Gespräch mit SPIEGEL ONLINE. Der Diensteanbieter stellt zum Ende des Jahres seine E-Mail-Angebote ein. Simon kapituliert vor den neuen Verpflichtungen nach der TKÜV - der Telekommunikations-Überwachungsverordnung.

Seit dem Ende des Bundespost-Monopols läuft die Telekommunikation der Bürger nicht mehr über den Staat selbst. Wollen Ermittler nun mitlauschen, müssen die Behörden erst einmal die ausgetauschten Inhalte in die Hände bekommen. Das geht nicht, ohne die Provider in die Pflicht zu nehmen.

http://www.spiegel.de/netzwelt/politik/0,1518,332998,00.html

Funktionen von S/MIME und PGP

- Digitale Unterschrift
  - der Text einer E-Mail (nicht das Subject) wird digital unterschrieben
  - hierdurch kann der Empfänger überprüfen, ob die E-Mail wirklich vom Autor ist
- Verschlüsselung einer Nachricht
  - der Text wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt
  - die Nachricht ist nur für den Empfänger lesbar

Beispiel PGP-Signierung


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Einen schönen guten Tag,

dieses ist eine Testnachricht

Freundliche Grüße,
  Jan Hennig
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iD8DBQFB3IBKkVdU5LglgWARAqiHAJ9269XoLotgCyXRP0G4f8CiJGeBsgCfWPRq
w4s3V3JYobG2ADg4/OiZqKs=
=GBhC
-----END PGP SIGNATURE-----
```

Beispiel PGP-Verschlüsselung


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

hQIOA4hIhG++ZF7MEAf/RMq6nAWxw4yjY8rh41+fVZg3zyEkiK2gC2M6sE3EOIXL
424pZ3FcVR/sd78ZxCKMlSF93In+ruNLS0m9juZf+6xFZbwBApQQE1mNyQcO0Lqx
5Suijs348opyXBp0sFQLElxaDz1wmOYywVRdH/nHFhbcGHGgE1Toq71TY7QWP4Al
pcpRZ5rM3aFHDcR9ydwe8M+WFipZXo/MMDuZQvcJIP6XL3d1N+3kpYJ6jhi4eEIN
q/dVEoyroTXyI31pMdawe2WbIw6IPtBQ6VCUbBxNn4Z282j6v03RubOsTcUflprx
zj0/vEBiJcnNHvv/aUThLBkieG+3SXeBoQa6jv2nbQf+Ms2jWwIyUj9IQC/BjcuG
oZEO6H4GEr/OqEDXehZDmMcoWMqmhdP3lthsrNYBtFlpE/Fx2qBXUce89m9gkveJ
vM7WNovojGv95UKE1LtRNQlNBuZ0fis9rVrwneNB0bzR0RjGEBFKjFINnqHaYkLk
MJLbUb7Ew/o+tonKIGydFZCfPnaqMCpX43MG2DvXw+uuzm2O3dyuYdqXbU4xg6dS
c2Fia4+MD8DzkqPbFtGvDKmnu3bx3046WyYccA+Fd7hYZNmg2CtfByeJbvex6Nof
m/DMc6RzPG/p2xW8r7PQgmYzGI9vvs30fH7mT6wsDYt9JzulkVG7Sq21KCsGothu
W9LAHwHggYfrrRqyO9D4dSSxYLdjodtzwr+ccR2yEYSV0raWDqgsoVe3nGeGGwzA
ev8hYComvRzPfyJTJEewWh1DI6mw3JCmqxwpfr/oYln/URtU+jtfEhbLwNh1ey2W
AqWRwlYYLH+l40q7NA0KyNURqfTq2+VqPil0ZQ8235uNiyqyA1sWMGCz7Lc6MniK
dNFLYEYQO4CPuj1NXLwJU25z48O07fcZP8mzJIjEA87Yc96BpqiUA5qauZtkrWYf
gkscXGsS5ntdiwoEe0v0WPriaepEi/I7h6o+yBmmdgFm7bk=
=ehvd
-----END PGP MESSAGE-----
```

Beispiel S/MIME-Signierung


```
Subject: Signierte Nachricht
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="---SKER9928983

This is MIME

-----SKER992898376--
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hallo Marcel,

dies ist eine signierte Nachricht, die ich mit dem Freemail Dienst von Web.de geschickt habe.

-----SKER992898376--
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIIFzgIBATEJMAcGBSsOAwIaMIAGCSqGSIb3DQEHAQAA
oIID+jCCA/YwggLeoAMCAQICAyuJWDANBgkqhkiG9w0BAQQFADCBoTELMAkGA1UE
...
LIPuTR9TMVRraE5MmGSFcmTynFrrfhGUP2IIy55zXl5OkrxqWjkMoBim0HyfOorR
98riKFFCmHoBQyN41mK7KgcAAAAA
-----SKER992898376----
```

Aussicht

Themenübersicht für die kommende Vorlesung:

- IMAP
- weitere Anwendungsprotokolle und -mechanismen

Ende Teil 12. Danke für die Aufmerksamkeit.