Internetdienste

Dr. Walter Ebner
Dr. Albert Weichselbraun

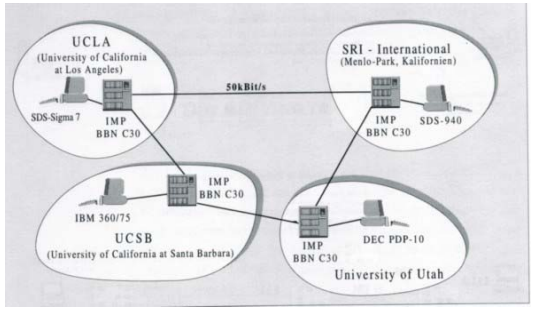
Wirtschaftsuniversität Wien

Inhalt

- Geschichte
- Client/Server
- WWW
- Telnet
- Mail
- FTP

Geschichte des Internets

- ARPANET - Advanced Research Project Agency 1.9.1969



Geschichte

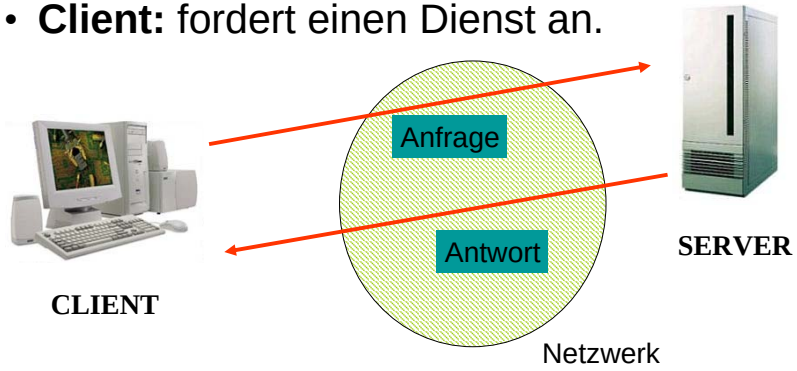
- 1972: 40 vernetzte Rechner
- Vorstellung auf der *First International Conference on Computer Communications*
- Gründung der *InterNetwork Working Group* zur Entwicklung eines gemeinsamen Übertragungsprotokolls =>1982 TCP/IP

Internetdienste

- Benutzen die Internet-Infrastruktur.
- Arbeiten meist nach dem Client-Server-Prinzip.
- Kommunikation zwischen Client und Server läuft nach streng festgelegtem Protokoll ab.
- WWW, FTP, Email, Telnet, News, ...

Client/Server Architektur

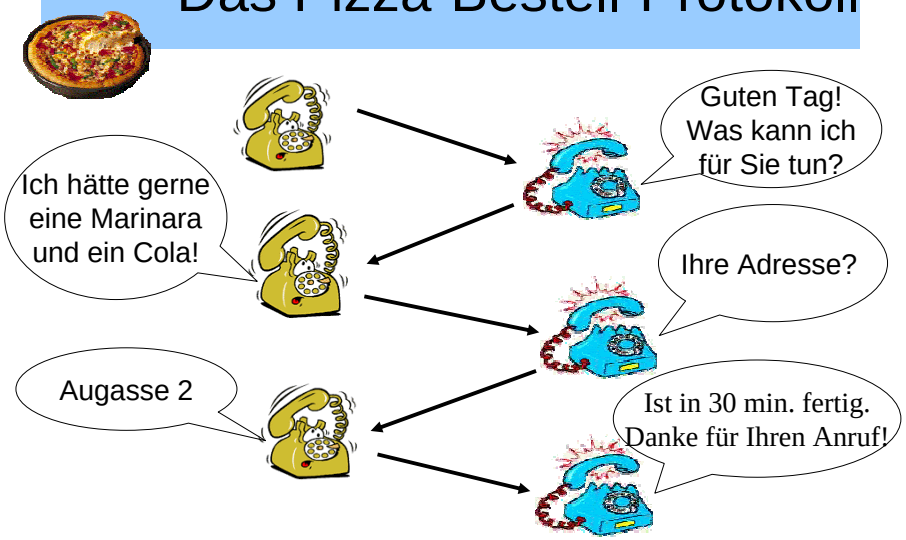
- **Server:** bietet einen Dienst an.
- **Client:** fordert einen Dienst an.



Protokoll

- Die Kommunikation nach dem Verbindungs-aufbau erfolgt nach strengen Regeln.
- Jeder Internetdienst hat eigene Regeln.
- Die Regeln für Internet-Protokolle sind in sogenannten RFCs (Request for Comments) niedergelegt.
- Bsp: RFC 821 - Simple Mail Transfer Protocol
  RFC 2616 – Hypertext Transfer Protocol 1.1

Das Pizza-Bestell-Protokoll



Telnet

- Telnet ist ein Protokoll, mit dem es möglich ist sich auf einem anderen Rechner im Netz einzuloggen und auf dem dann zu arbeiten.
- Dazu muss man jedoch einen Account auf dem jeweiligen Rechner haben.
- Syntax: **telnet *hostname***
  z.B.: telnet gutemine.wu-wien.ac.at
- SSH-Protokoll: Funktioniert gleich wie Telnet, nur sind die Daten während der Übertragung verschlüsselt (ist somit sicherer).

Das World Wide Web

Das WWW ist ein über das Internet abrufbares Hypertext-System.
Wesentliche Komponenten:

- Dokumentenbeschreibungsspache **HTML**=Hypertext Markup Language aufbauend auf **SGML**= Standard Generalised Markup Language.
- Erlaubt die Vernetzung von Dokumenten durch Verwendung von **Links** von beliebigen Stellen eines Dokuments auf beliebige Stellen anderer Dokumente.
- **URL**‘s (Uniform Resource Locator) als Standardadressen für Ziele von Links, z.B.:
  http://www.wu-wien.ac.at/usr/ebner/index.html
- **HTTP** = **Hypertext Transfer Protocol** als Standardprotokoll für den Zugriff und die Übertragung von Dokumenten.
- **Browser** (Mosaic/Netscape seit 1993/94) zur Visualisierung von HTML-Dokumenten und Abwicklung der Zugriffe auf Dokumente mittels HTTP.

Standardisierung des WWW

- Gründung des **World Wide Web-Consortiums W3C** im Jahr 1994 mit dem Ziel der internationalen Standardisierung von Funktionen, Sprachen und Diensten im World Wide Web.
- Informationen zu allen wesentlichen Standards des WWW verfügbar über die Homepage des W3C: http://www.w3.org/

Dienste lokalisieren mit DNS

- DNS hilft beim Auffinden verschiedener Dienste
  => Unterschiedliche Typen von DNS-Einträgen

Typ	Bezeichnung	Verwendung
A	Hosteintrag	IP-Adresse eines Rechners
CNAME	Canonical name	Alias Name
MX	Mailexchanger	Name des zuständigen Mailservers
NS	Nameserver	Name des zuständigen Nameservers
TXT	Text	Zusätzliche Informationen zur Domaine

DNS Abfragen mit “dig“

- “dig” ist **das** Standardtool zum Abfragen von DNS Informationen
- Syntax:
  dig [@nameserver] [Typ] dnsname
- zum Beispiel

```
dig @ns1.univie.ac.at ns wu-wien.ac.at

;; AUTHORITY SECTION
wu-wien.ac.at.10800 IN NS ns2.wu-wien.ac.at.
wu-wien.ac.at.10800 IN NS ns5.wu-wien.ac.at.
wu-wien.ac.at.10800 IN NS ns1.wu-wien.ac.at.
```

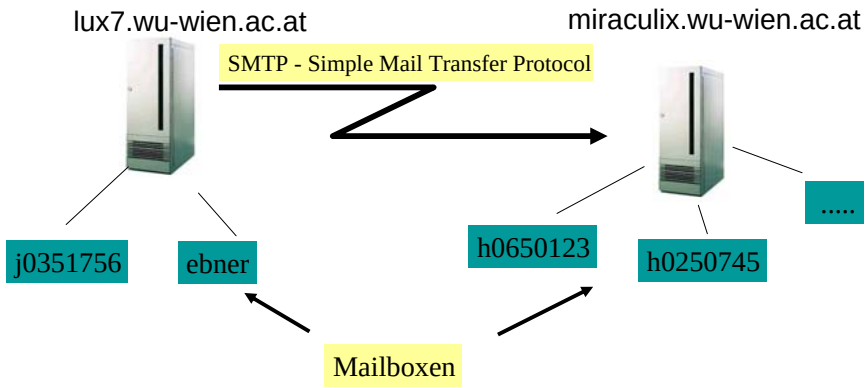
Übungsbeispiel

- Ermitteln Sie die IP-Adresse des Nameservers für die Domäne chello.at.
- Wie lauten die Nameserver für die Domäne atnet.at?
- Wie lauten die IP-Adresse(n) der Server, auf welchen sich die ORF-Homepage befindet?
- Welche Information enthält das Textfeld von .atnet.at?

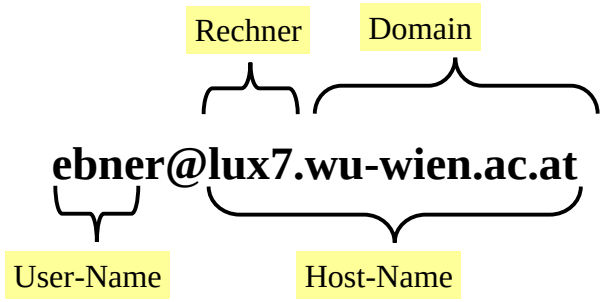
E-Mail

- Ermöglicht das Übersenden von elektronischen Nachrichten.
- Zum Versenden wird SMTP (Simple Mail Transfer Protokoll) verwendet.
- Durch MIME-Extensions Attachments möglich.

E-Mail



E-Mail Adressen



Aufbau einer E-Mail

- Der Header einer E-Mail enthält Angaben, die zum Versenden der E-Mail benötigt werden.
- Der Body enthält den Text der Nachricht.
- Zusätzlich können Dateien als Attachment angehängt werden.

SMTP Transaktion

albert@miho:~/tmp$ telnet mx1.atnet.at 25

220 smtp.atnet.at ESMTP
ehlo miho.ai.wu-wien.ac.at
250-smtp.atnet.at
250-STARTTLS
250-PIPELINING
250-8BITMIME
250 AUTH LOGIN PLAIN CRAM-MD5
mail from: aweichse@ai.wu-wien.ac.at
250 ok
rcpt to: albert@atnet.at
250 ok

SMTP Transaktion

data
354 go ahead
From: Albert Weichselbraun <albert@iaeste.at>
To: Albert Weichselbraun <albert@atnet.at>
Subject: Testmessage

Die erste Zeile der Nachricht.
.
250 ok 1158651671 qp 1576

Header einer E-Mail

- Absender (From)
- Empfänger (To)
- Betreff (Subject)
- Kopie (CC, carbon copy)
- Kopie (BCC, blind carbon copy)

Mail Clients

Bieten ein benutzerfreundliches Interface.

- Online - Clients: elm, pine
- Offline – Clients: Mails werden über POP (Post Office Protocol) oder IMAP heruntergeladen.

  MS Outlook, Eudora, Pegasus, ...
- Webmail: z.B: IMHO, IMP

Online Mail Clients: Pine, Elm

- E-Mails werden direkt auf dem Mailbox-Rechner geschrieben und gelesen.
- Telnet zum Mailhost (z.B. telnet miss.wu-wien.ac.at)
- Elm mit **mail** oder **elm** starten.
- Pine mit **pine** starten:
  - Editor ist ähnlich zu pico
  - Mail-Archivierung in Foldern
  - Anbindung von Attachments möglich.

POP/IMAP Mail Clients

- POP (Post Office Protocol): auch offline verwendbar
- Lädt E-Mails vom zenralen Server herunter.
- IMAP (Internet Mail Access Protokoll)
  -> E-Mails verbleiben am Server
- **Beispiele:** Mozilla Thunderbird, MS Outlook, Pegasus, Evolution, ...

IMP Webmail

- Webmail Client der WU-Wien:
  https://webmail.wu-wien.ac.at/horde/

FTP – File Transfer Protocol

- Bezeichnet ein Protokoll, mit dem Dateien von einem Rechner zu einem anderen transferiert werden können.

ftp *hostname*

Befehle: get/put/ls/quit/help

FTP - File Transfer Protocol

- Anmeldung mit Benutzername und Passwort.
- Anonymer FTP-Zugriff mit

  Username: *anonymous*

  Passwort:*email-Adresse*

FTP zwischen 2 Servern

- Übertragung einer Datei zwischen zwei Servern:

ftp idefix.wu-wien.ac.at
Username +Password eingeben
mit cd *Verzeichnis* in das gewünschte Verzeichnis auf idefix wechseln.
put brief.txt
quit

Grafischer FTP-Client

- Übertragung einer Datei zwischen einem Windows-PC und einem Server:

Ein lokales FTP-Programm verwenden. Schaut wahrscheinlich ähnlich aus wie dieses hier, muss es aber nicht!

Angriffszenarien

- “Man in the middle Attack“
  - Ein Host fängt die Kommunikation ab (Vergleiche Traceroute)
  - Gegenmaßname: SSL/gnupg/PGP
- Phishing
  - Gefälschte E-Mails/Webseiten
  - Gegenmaßnahmen: One Time Passwords, Externe Crypt-Devices (Chipkarte)
- Keylogger
  - Gegenmaßnahmen: One Time Passwords
- Kompromitierter Rechner

Übungsaufgabe

- Beantragen Sie eine Homepage an der WU
- Laden Sie sich irgendein Bild aus dem Internet herunter.
- Übertragen Sie dann diese Datei in das Verzeichnis Ihrer Homepage (public_html) auf Ihren Powernet-Rechner (asterix, zechine, maestria, ...)
- Betrachten Sie das Bild in einem Browser (Über den URL der Homepage, nicht das lokale Bild)

Übungsaufgabe

- Ermitteln sie den NS, MX und A Record für heise.de
- Erklären sie die dig-Ausgabe für das obige Beispiel.
- Der heise-Verlag entschließt sich dazu den Mailserver umzustellen. Wie lange kann es maximal dauern, bis alle Server im Internet den neuen Mailserver verwenden?

Übungsaufgabe*

- Senden Sie ein E-Mail mit
  - Absender: president@us.gov
  - Subjekt: Weltherrschaft
  - an aweichse@ai.wu-wien.ac.at
- SPF, Signatures & Encryption, gpg, pgp
- Mozilla Plugin -> Enigma

PGP/GnuPG

- PGP = Pretty Good Privacy
- Ermöglicht das
  - Signieren und
  - Verschlüsseln von Nachrichten und Dateien
- Freie Version von PGP = GnuPG
- Unterstützt **symetrische** und **asymetrische** Verschlüsselung
- Verschieden grafische Frontends (zum Beispiel Enigma für Thunderbird) verfügbar.

PGP/GnuPG

- Vorgangsweise: asymetrische Verschlüsselung
  - beim ersten Mal muss das Schlüsselpaar (Public + Private Key generiert werden)

    ```
    gpg –gen-key
    ```
  - anschließend den privaten Schlüssel mit
    `gpg –send-keys`
    auf den Keyserver exportieren.
  - Verschlüsseln einer Nachricht
    `gpg –encrypt nachricht`
  - die verschlüsselte Datei wird in nachricht.asc abgelegt und kann mit
    `gpg –decrypt nachricht.asc`
    wieder entschlüsselt werden.

PGP/GnuPG

- Vorgangsweise: signieren einer Nachricht
  - Voraussetzung: existierender privater Schlüssel
  - Die Nachricht kann mit
    `gpg –clearsign nachricht`
    unterschrieben werden.
  - Signatur überprüfen:
    `gpg –verify nachricht.asc`

Übungsaufgabe*

- Erstellen Sie ein PGP/GnuPG Schlüsselpaar
- Erstellen Sie eine Nachricht mit Ihrem Namen, Matrikelnummer und Geburtsjahr und signieren Sie diese mit Ihren Schlüssel
- Verschlüsseln Sie die Nachricht, sodass diese nur von albert.weichselbraun@wu-wien.ac.at gelesen werden kann.