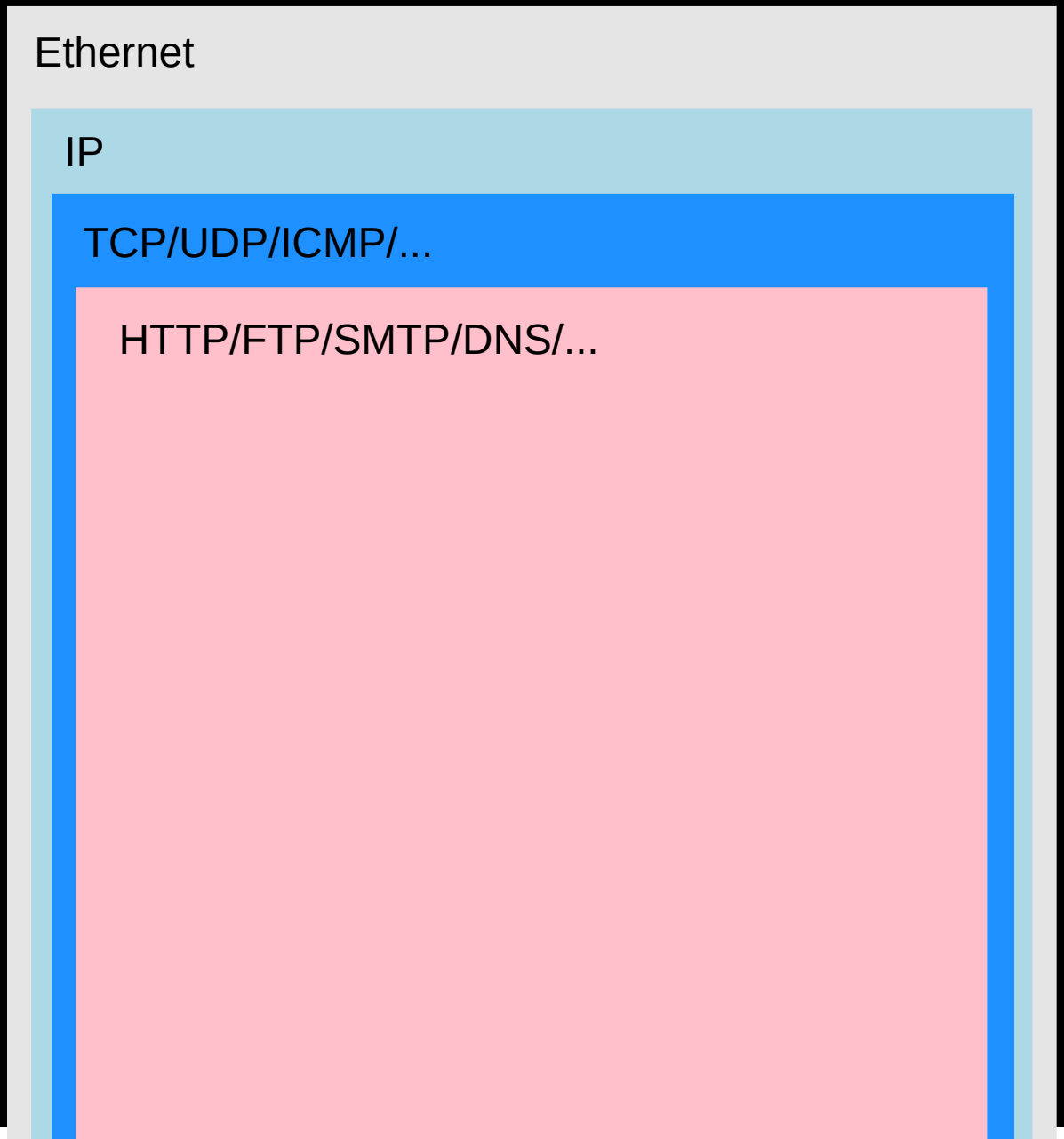
Networking - Überblick

TCP, UDP, ICMP

René Pfeiffer
Systemadministrator GNU/Linux Manages!
lynx@luchs.at
rene.pfeiffer@paradigma.net

TCP, UDP, ICMP & andere Protokolle

Die dritte Netzwerkschicht



TCP

Transmission Control Protocol

- primär eingesetzt bei Datentransport
- HTTP, FTP, SMTP, POP3, etc.

TCP - Eigenschaften

- verbindungsorientiert
  - expliziter Verbindungsaufbau und -abbau
- zuverlässig
  - Reihenfolge der Daten wird berücksichtigt
  - Checksummen für Daten
- stetiger Datenstrom

TCP - Ports

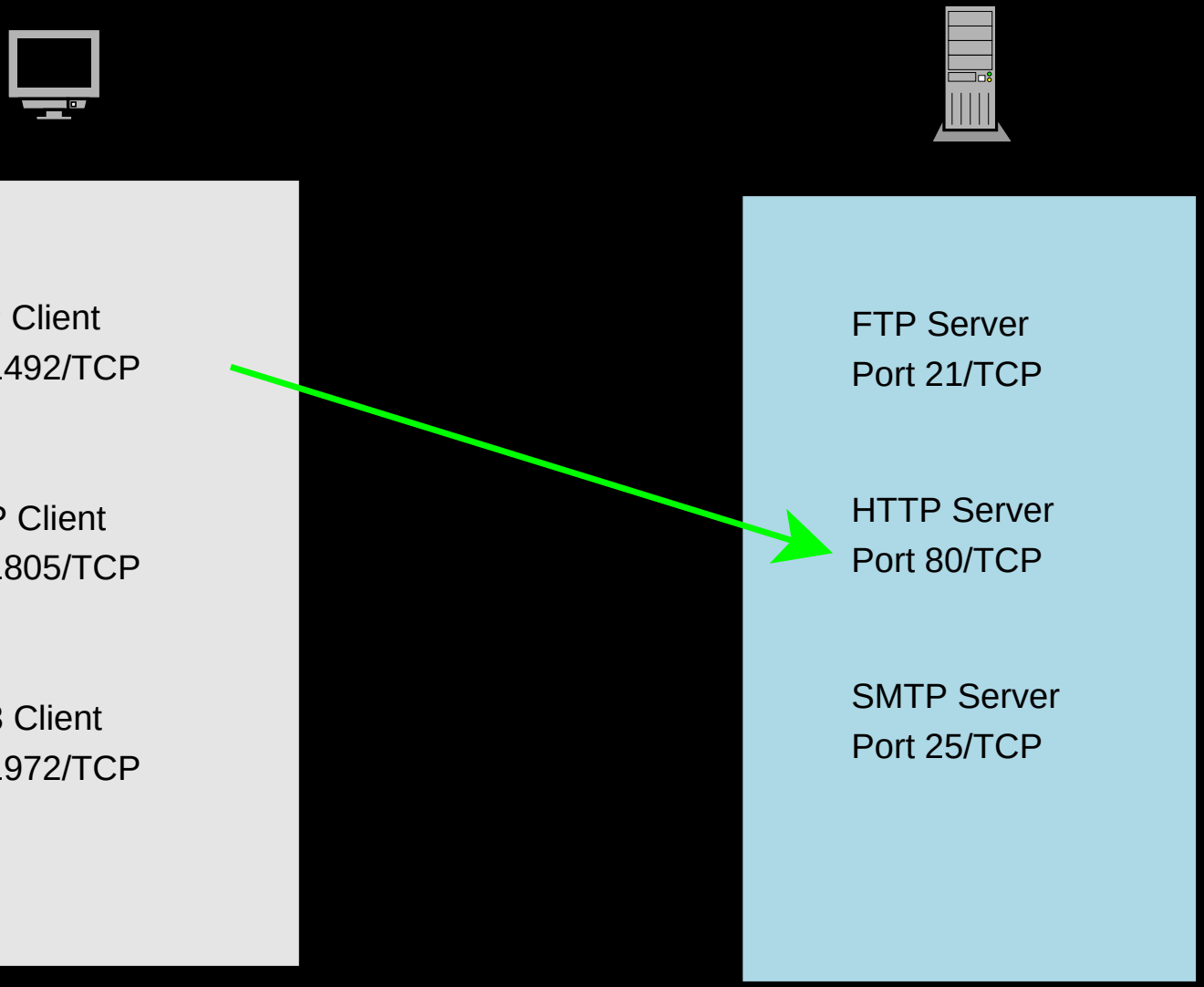
- Ports dienen dazu verschiedene Applikationen auf einem Server zu kontaktieren.
- Ports reichen von 1 bis 65535
  - Ports 1-1023 sind "privilegierte Ports"

Socket - Begriff für eine Kombination aus IP-Adresse und Port
83.133.48.95:80

.

Eine Verbindung zu einem HTTP-Server

Sockets identifizieren die Verbindung eindeutig



TCP-Pakete im Detail

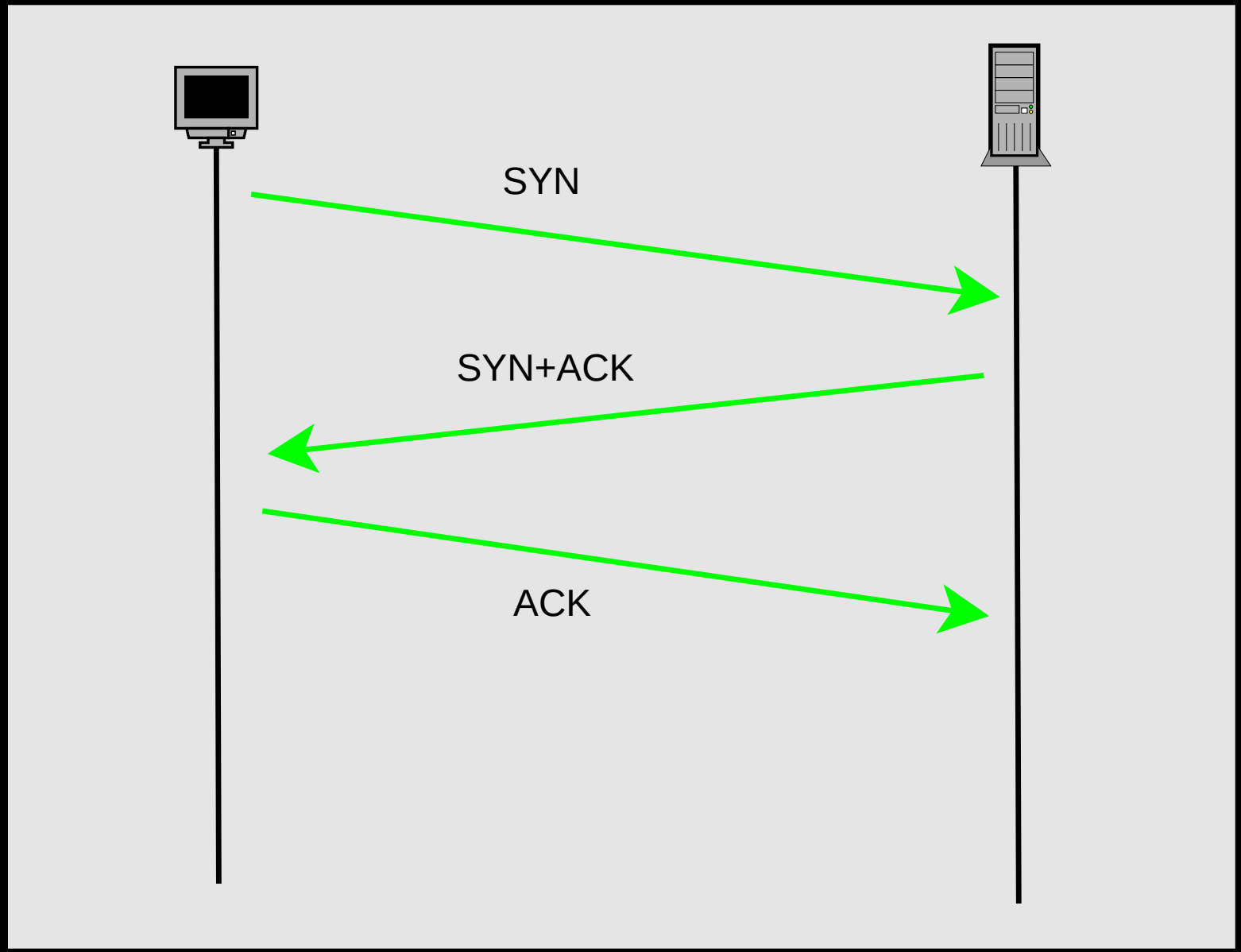
Auch auf TCP-Ebene werden Daten nur als Pakete verschickt.

- Source Port
- Destination Port
- TCP Flags
  - SYN - Synchronization; Verbindungsaufbau
  - ACK - Acknowledgement
  - FIN - Finish; leitet Verbindungsende ein
  - RST - Reset; Verbindungsabbruch
- TCP Checksumme
  - Checksumme über Kopfdaten und Daten

Danach folgen die Daten der nächsten Schicht.

Aufbau einer TCP-Verbindung

Three Way Handshake



UDP

User Datagram Protocol

Wird verwendet für

- Streaming
- zeitkritische Applikationen
- bei sehr kleinen Datenmengen

UDP - Eigenschaften

- paketorientiert
  - keine Verbindungen
- unzuverlässig
  - keine Fehlerkorrektur durch Retransmission
- kein stetiger Datenstrom

"Send & Pray!"

UDP - Ports

- ganz analog zu TCP Ports
- UDP Ports kollidieren nicht mit TCP Ports

UDP-Pakete im Detail

- Source Port
- Destination Port
- Checksumme über Daten und Kopfdaten

ICMP

Internet Control Message Protocol

- dient zum Übertragen von Fehler- und Diagnosemeldungen

ICMP-Pakete im Detail

- ICMP Type
  - Art der Nachricht
- ICMP Code
  - genauerer Status- oder Fehlercode
- Checksumme über gesamtes Paket

ICMP Typen und Codes

- echo request - Aufforderung zum Senden eines echo reply
- echo reply - Antwort auf echo request

- destination unreachable - Netzwerk oder Host nicht erreichbar

- source quench - Zielrechner bittet Paketrate zu drosseln

- time exeeded - TTL eines Paketes abgelaufen, Paket wurde gelöscht

- parameter problem - Fehler in Kopfdaten oder allgemeiner Fehler

- destination administratively prohibited - Netzwerk verboten

ICMP Echo Request

Spielereien mit ping

```
lynx@nightfall:~/$ ping -c 10 xaos.pvl.at
PING xaos.pvl.at (194.152.160.154) 56(84) bytes of data.
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=1 ttl=244 time=12.8 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=2 ttl=244 time=9.57 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=3 ttl=244 time=10.3 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=4 ttl=244 time=8.62 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=5 ttl=244 time=22.0 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=6 ttl=244 time=9.37 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=7 ttl=244 time=8.77 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=8 ttl=244 time=9.21 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=9 ttl=244 time=10.8 ms
64 bytes from xaos.pvl.at (194.152.160.154): icmp_seq=10 ttl=244 time=8.78 ms

--- xaos.pvl.at ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 8.625/11.053/22.070/3.868 ms
lynx@nightfall:~/$
```

Applikationsschicht

Die vierte Netzwerkschicht (DNS, SMTP, POP3, IMAP, HTTP, HTTPS, etc.)

DNS - Domain Name System

Namen haben Macht

System zum Abbilden von Namen auf IP-Adressen (und umgekehrt)

riesige verteilte Datenbank

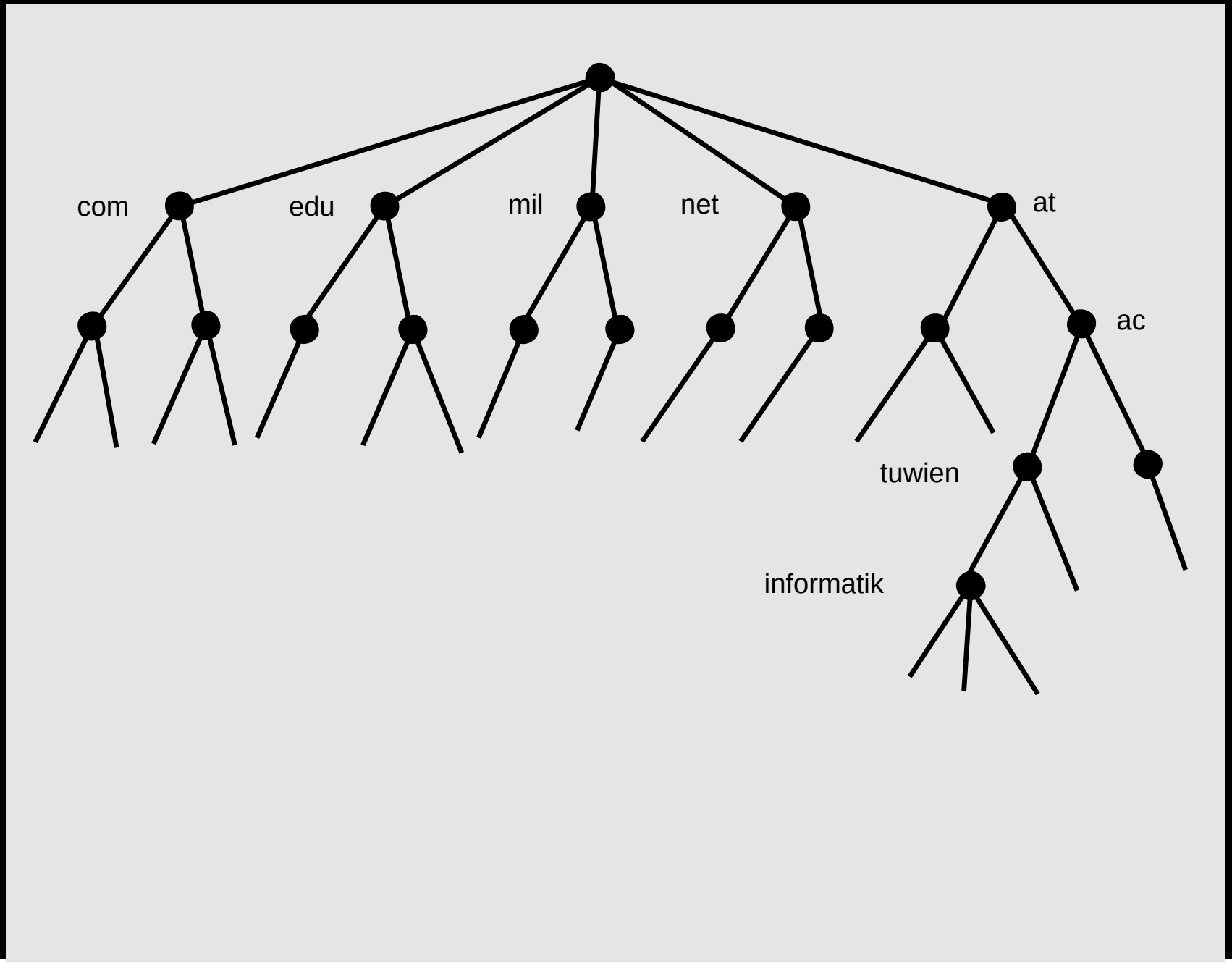
Geschichte des DNS

- Datei hosts.txt auf allen vernetzten Rechnern
  - Verwaltung der hosts.txt durch SRI-NIC am Stanford Research Institute
- Meldungen über neue Einträge an zentrale Stelle
- Implementation des DNS im Jahre 1984 (im alten ARPAnet)
  - Dezentrale Verwaltung der Domain Name Daten

Beispiele aus dem Namensraum des DNS

www.sae.edu
web.luchs.at
alfie.ist.org
news.bbc.co.uk
my-hostname-is-longer-than-yours.mit.edu
buero.gibts.net
cr.yp.to
www.insecure.org

Der Domain Name Space



Domain Name Space

Begriffe

- Top Level Domain (TLD)
  - edu, com, gov, mil, net, org, int, at, de, name, biz, info, ...
- Second Level Domain
  - sae.edu, luchs.at, bbc.co.uk, help.gv.at, ...
- Domain
  - ein Teilbaum des Domain Name Space
- Subdomain
  - ein Teilbaum einer Domain
- Nameserver
  - ein Server, der Informationen über Domains speichert und via DNS zur Verfügung stellt

Dezentrale Verwaltung durch Delegation

Ein Nameserver ist nur eine Autorität für seine Zone

Die Zonen root, at, ac.at und univie.ac.at

FIXME! Graphics!

Die Zonen root, com und dnsreport.com

FIXME! Graphics!

Die Zonen root, at, ac.at, tuwien.ac.at und informatik.tuwien.ac.at

FIXME! Graphics!

Zonen alle zusammengenommen

FIXME! Graphics!

Name Resolution

Funktionsweise von DNS Abfragen

Client fragt lokalen Nameserver nach IP für www.sensenmann.at
Nameserver fragt root Server
root Server verweist auf .at Server
Nameserver fragt .at Server
.at Server verweist auf sensenmann.at Server
Nameserver fragt sensenmann.at Server
sensenmann.at Server gibt die Auskunft 213.129.239.205

lokaler Nameserver gibt 213.129.239.205 an Client

.

DNS Caching

Zwischenspeichern von DNS Informationen

- jeder DNS Eintrag hat eine Lebensdauer (TTL)
- erst nach Ablauf der Lebensdauer fragen Nameserver erneut an
- wesentlich beschleunigte Abfragen

DNS Lookups selbst gemacht

Der Command Line Tool dig

```
lynx@nightfall:~$ dig www.sensenmann.at

; <<>> DiG 9.2.4rc5 <<>> www.sensenmann.at
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21447
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.sensenmann.at.             IN      A

;; ANSWER SECTION:
www.sensenmann.at.      43200   IN      A       213.129.239.205

;; AUTHORITY SECTION:
sensenmann.at.          43200   IN      NS      gilean.luchs.at.
sensenmann.at.          43200   IN      NS      majere.luchs.at.
sensenmann.at.          43200   IN      NS      dns1.akis.at.

;; ADDITIONAL SECTION:
dns1.akis.at.           11359   IN      A       213.129.244.66
gilean.luchs.at.        11359   IN      A       62.116.64.105
majere.luchs.at.        11359   IN      A       213.229.56.67

;; Query time: 46 msec
;; SERVER: 195.34.131.180#53(195.34.131.180)
;; WHEN: Thu Sep 16 01:56:13 2004
;; MSG SIZE  rcvd: 171

lynx@nightfall:~$
```

Electronic Mail (EMail)

SMTP, POP3, IMAP und Nachrichten

EMail ist schon über 30 Jahre alt.

EMail ist eine der kritischsten Anwendungen des Internets.

Aufbau von EMails

Briefumschlag und Brief

Absender
From: René Pfeiffer <lynx@luchs.at>

Empfänger
To: Member Support <members@digitalblasphemy.com>

Carbon Copy (Durchschlag)
Cc: lynx@anubis.luchs.at

Blind Carbon Copy ("geheimer" Durchschlag)
Bcc: sent-mail@anubis.luchs.at

Betreffzeile
Subject: Forgot my password

.

Inhalt von EMails

Kodierungen und Zeichensätze

- EMail ist ein textbasiertes Medium (US-ASCII-Text)
- zunehmende Internationalität hat zu Erweiterungen geführt
- MIME (Multi-purpose Internet Mail Extension)
  - erlaubt das Verpacken von allen Datenformaten
  - erlaubt internationale Zeichensätze

Transport von EMails

Wie kommt die Brieftaube zum Brief?

FIXME! Graphics!

Zugriff auf Mailboxen

oder wie die Taube letztlich landet.

- Post Office Protocol 3 (POP3)
  - Mails können nur als ganzes dem Mailprogramm gegeben werden
  - Mails können am Server gelöscht oder behalten werden
- Internet Message Access Protocol (IMAP)
  - effizienterer Zugriff auf Mails am Server
  - IMAP-Server scannt nur Header für Überblick
  - Verwalten von Mails am Server durch Ordner

File Transfer Protocol (FTP)

Datentransfer zwischen vernetzten Rechnern

FTP-Server erreicht man über TCP Port 21

FTP kann

- Dateien vom Server zum Client kopieren
- Dateien vom Client zum Server kopieren
- Ordner erstellen
- Dateien und Ordner umbenennen oder verschieben

neben einigen anderen Funktionen.

File Transfer Protocol (FTP)

Eigenheiten von FTP

- FTP ist älter als das IP
- FTP kennt verschiedene Übertragungsmodi
  - binär für Binärdaten
  - ascii für Textdaten
- FTP benutzt immer zwei TCP-Verbindungen
  - Kommandokanal mit TCP Port 21
  - Datenkanal auf variablen Ports
- Aktives FTP
  - Server eröffnet Datenkanal zum Client
- Passives FTP
  - Client eröffnet Datenkanal zum Server

Hyper-Text Transfer Protocol (HTTP)

World Wide Web

Server sind üblicherweise auf TCP Port 80 zu finden

HTTP Requests

Wo gibt es Neuigkeiten?

Im HTTP bestimmten URLs (Uniform Resource Locators) die Quelle

- http://www.univie.ac.at/
- http://www.slac.stanford.edu/
- http://www-306.ibm.com/software/lotus/support/organizer/support.html
- http://www.vamp.org/Gothic/Text/gothlist.html
- http://web.luchs.at/article.php?cat=6&aid=166
- http://derstandard.at/?id=1795154

HTTP Requestmethoden

Browser/Server Kommunikation

- GET Request
  - Client fordert Daten an
  - Client kann beim Anfordern aber auch Daten mitschicken
  - http://web.luchs.at/article.php?cat=6&aid=166
- POST Request
  - Client schickt Daten an Server
  - Daten in URL nicht sichtbar
- HEAD Request
  - Client fordert nur HTTP Header an

Sowohl GET wie POST können Daten aus einem HTML Formular an den Webserver übertragen.

HTTP Header

HEAD Requests in Aktion

```
lynx@nightfall:~$ HEAD http://www.server.at/
200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Thu, 16 Sep 2004 23:37:05 GMT
Pragma: no-cache
Server: Apache/1.3.31 (Unix) mod_ssl/2.8.17 OpenSSL/0.9.7a
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Client-Date: Thu, 16 Sep 2004 23:38:43 GMT
Client-Peer: 195.230.63.210:80
Client-Response-Num: 1
Set-Cookie: PHPSESSID=637dbbe829cf432bff88e65217932ea5; path=/
lynx@nightfall:~$
```

HTTP Response Codes

Webserverantworten

- 100-199 nur informative Meldungen, sehr selten
- 200-299 Request war erfolgreich
- 300-399 Warnmeldung, Request war erfolgreich
- 400-499 Client Error (fehlerhafter Request)
- 500-599 Server Error (Request war gültig)

HTTP Feinheiten

Verbesserungen

HTTP 1.1 kennt HTTP Pipelining

pro Webseite wird nur eine TCP Verbindung gebraucht

alle Elemente der Seite gehen dann über diese eine Verbindung

HyperText Transfer Protocol Secure (HTTPS)

Verschlüsseltes HTTP

funktioniert analog zu HTTPS

verwendet TCP Port 443

URLs bleiben fast gleich:

- https://www.ccc.de/
- https://listman.redhat.com/archives/ataraid-list/2004-September/msg00006.html

Secure Shell (SSH)

Verschlüsselte Remote Shell