Systeme II

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Sommersemester 2006

23. Vorlesung

26.07.2006

schindel@informatik.uni-freiburg.de

IPv4 versus IPv6

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Prefixes

	IPv6	V6 Net	6Bone	IPv4	IPv4 / IPv6
Prefix Count	708	704	4	190524	190524 / 708

Addresses

	IPv6	V6 Net	6Bone	IPv4	IPv4 / IPv6
Announced Address Span	17.3215	17.3653	22.3853	1.46711905	1.46711905 / 17.3215
Announced % of Total Address span	0.000611	0.000592	0.000018	36.170387	36.170387 / 0.000611
Average Address Span per Announcement	26.7891	26.8248	24.3853	19.0069	19.0069 / 26.7891
Average Announcement Length	34.2302	34.2827	25.0000	22.2430	22.2430 / 34.2302

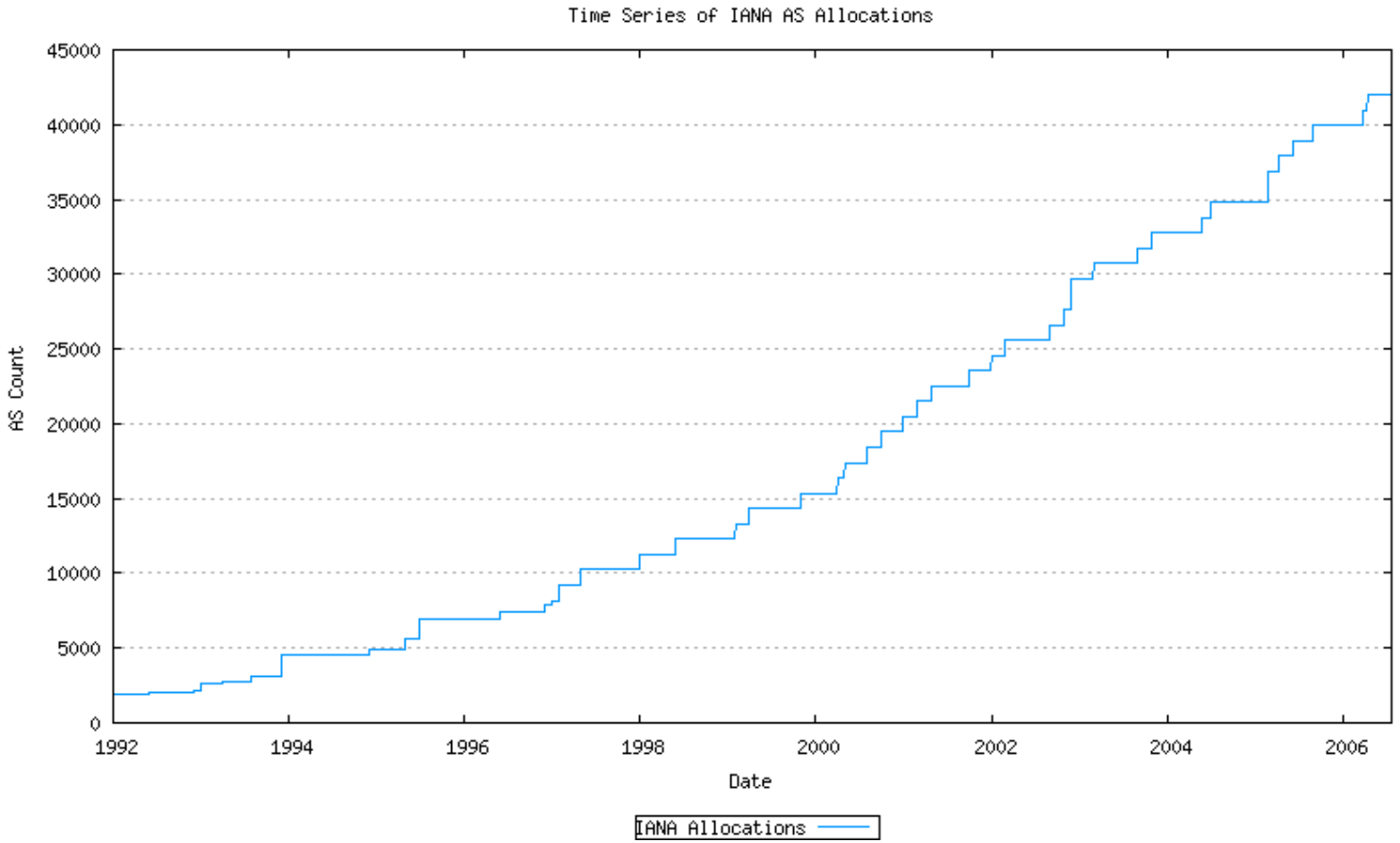
AS Numbers

	IPv6	V6 Net	6Bone	IPv4	IPv4 / IPv6
AS Count	598	598	10	22612	22612 / 598
Origin-only ASes	433	433	2	15925	15925 / 433
Origin and Transit ASes	150	150	2	6616	6616 / 150
Transit ASes	15	15	6	71	71 / 15
ASs Announcing a single prefix	519	521	2	9481	9481 / 519
Average Announcements per AS	1.2144	1.2075	1.0000	8.4523	8.4523 / 1.2144
Average Address Range per AS (prefix)	26.5089	26.5527	24.3853	-	8.4523 / 26.5089
Max Announcments for an AS	23	23	2	1450	1450 / 23
Max Announced span for an AS	19.00	19.00	23.00	-	1450 / 19.00

http://bgp.potaroo.net/v6/v6rpt.html

Exponentielles Wachstum des Internets

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

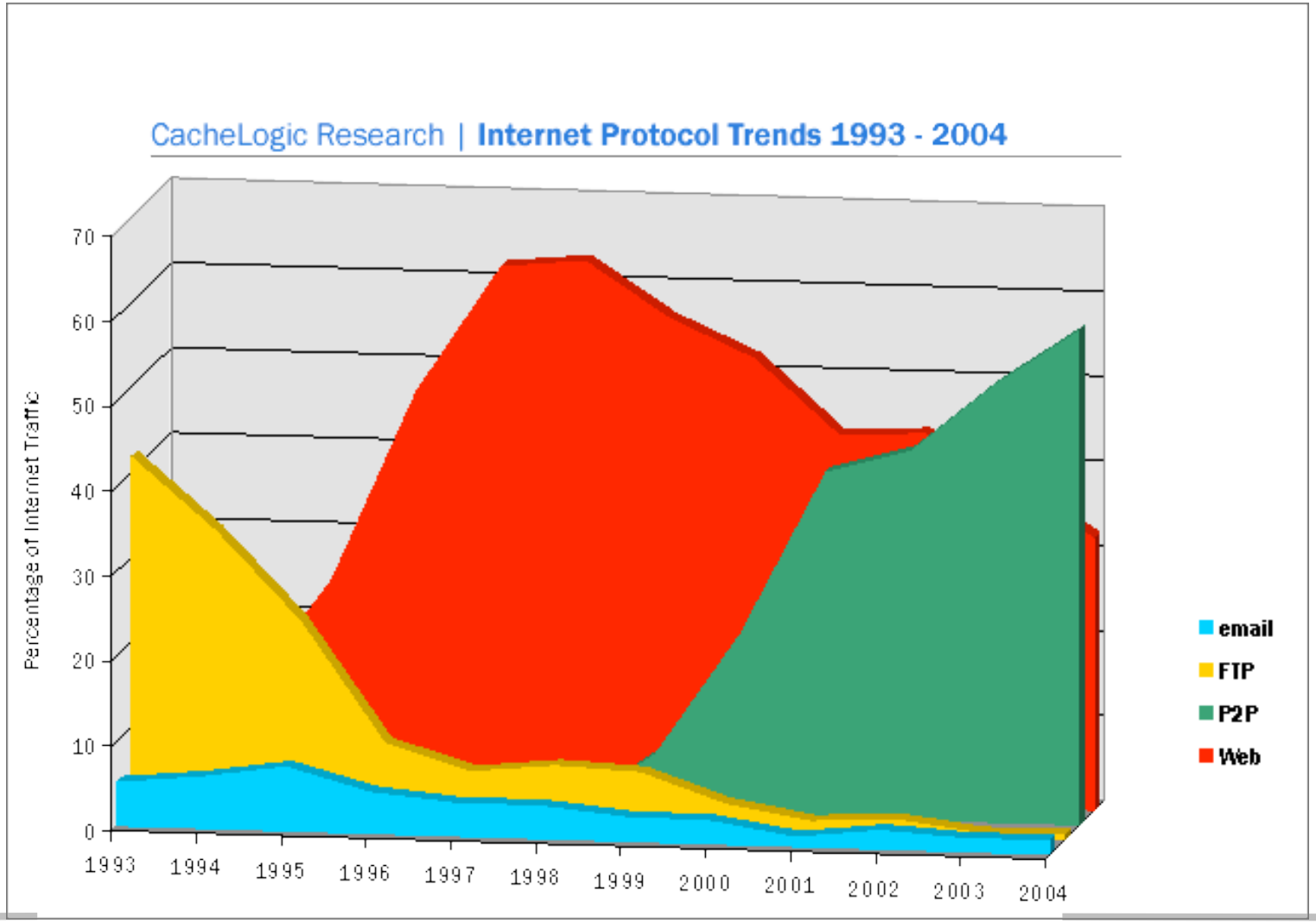


http://www.potaroo.net/tools/asns/

Verkehr im Internet

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

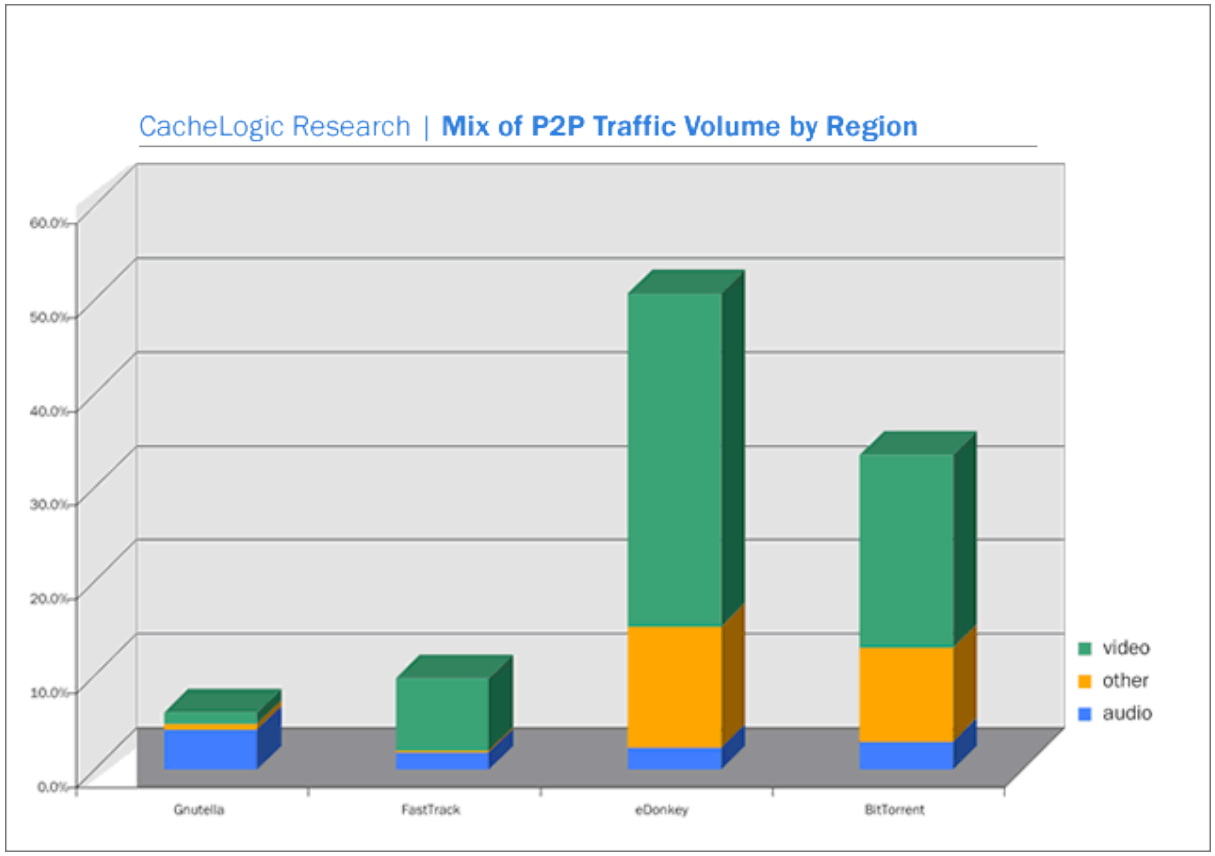
- **http://www.cachelogic.com/research/2005_slide07.php#**



P2P dominiert das Internet (Stand 2004)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

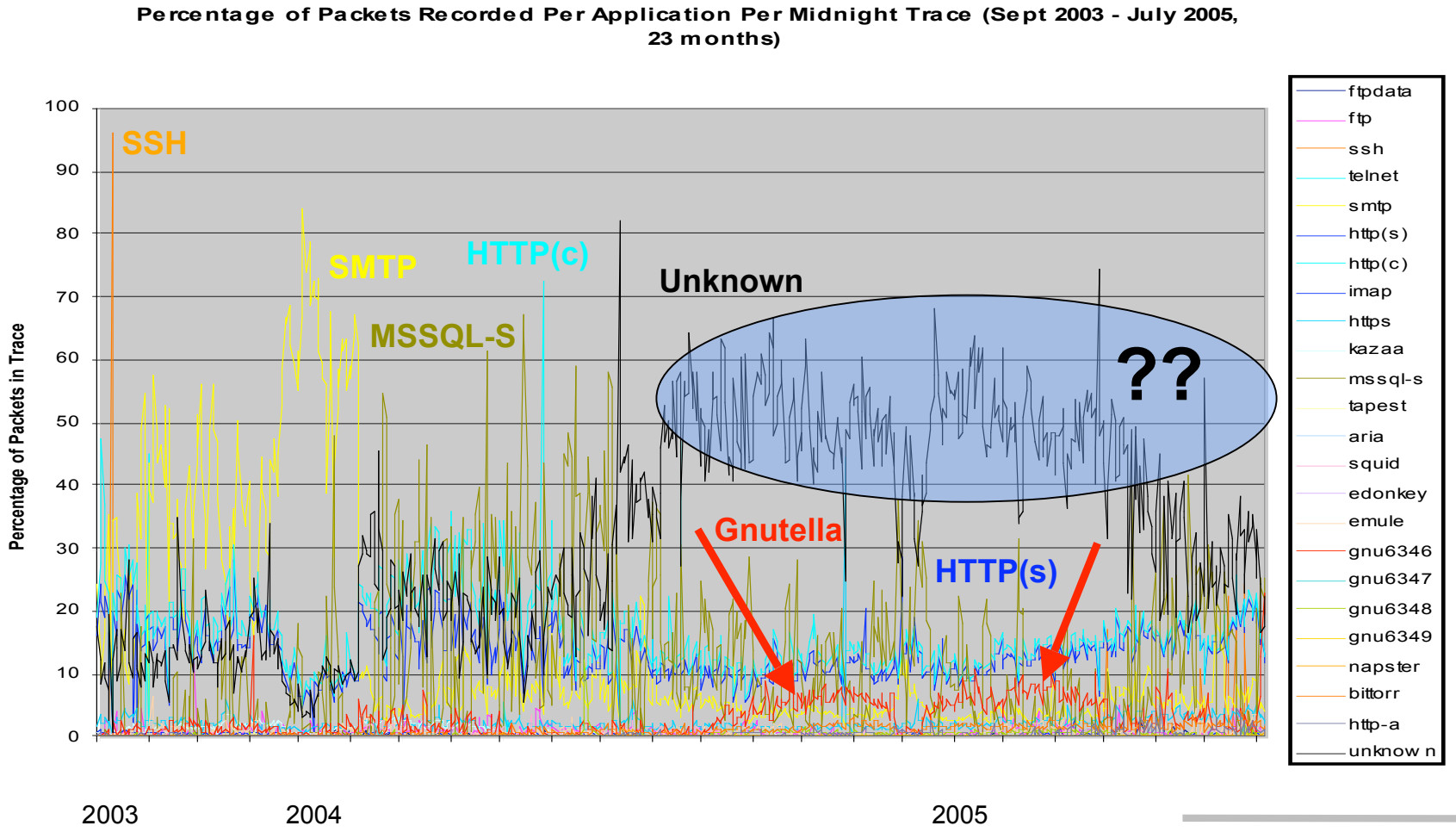
- **Haupt-Protokolle**
  - eDonkey
  - BitTorrent
  - FastTrack
  - Gnutella



Analyse des Verkehrs schwierig

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Aus Master Thesis-Vortrag von Alok Madhukar**
  - Port-Analyse des nächtlichen Verkehrs einer kalifornischen Universität



Was ist ein Peer-to-Peer-Netzwerk?

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Was ist ein Peer-to-Peer-Netzwerk nicht?**
  - Ein Peer-to-Peer-Netzwerk ist kein Client-Server-Netzwerk!
- **Definition**
  - *Peer-to-Peer*
    - bezeichnet eine Beziehung zwischen gleichwertigen Partnern
  - *P2P*
    - Internet-Slang für Peer-to-Peer
  - Ein *Peer-to-Peer-Netzwerk* ist ein
    - Kommunikationsnetzwerk zwischen Rechnern im Internet
    - in dem es keine zentrale Steuerung gibt
    - und keine zuverlässigen Partner.

Napster

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Shawn (Napster) Fanning**
  - brachte Juni 1999 eine Beta-Version seines mittlerweile legendären Napster-Peer-to-peer-Netzwerks heraus
  - Ziel: File-sharing-System
  - Tatsächlich: Musik-Tauschbörse
  - Herbst 1999 war Napster Download des Jahres

- **Urheberrechtsklage der Musik-Industrie im Juni 2000**

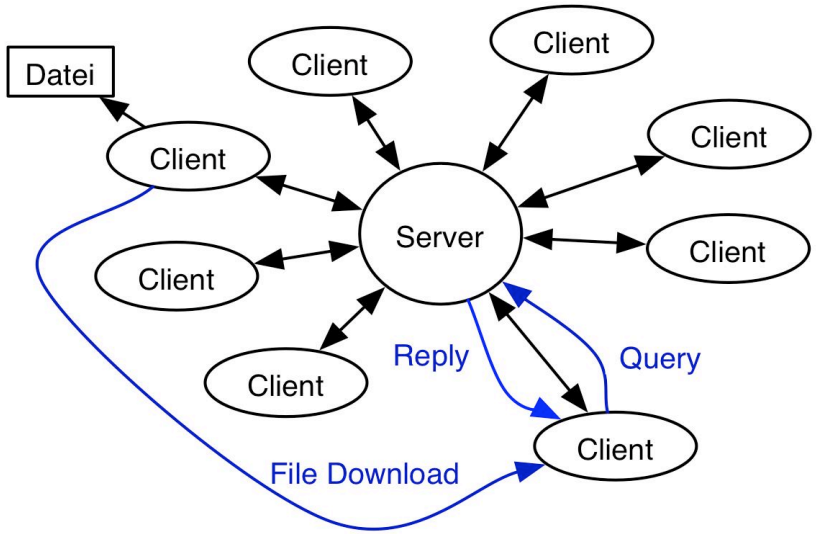
- **Gegen Ende 2000 Kooperationsvertrag**
  - zwischen Fanning mit Bertelsmann Ecommerce
  - auch juristisch gescheitert

- **Seit 2001 ist Napster eine kommerzielle File-Sharing-Plattform**

Wie funktioniert Napster?

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Client-Server-Struktur**
- **Server unterhält**
  - Index mit Meta-Daten
    - Dateiname, Datum, etc
  - Tabelle der Verbindungen der teilnehmenden Clients
  - Tabelle aller Dateien der teilnehmenden Clients
- **Query**
  - Client fragt nach Dateinamen
  - Server sucht nach passenden Teilnehmern
  - Server antwortet, wer die Datei besitzt
  - Anfrage-Client lädt Datei von datei-besitzenden Client herunter



Gnutella - Geschichte

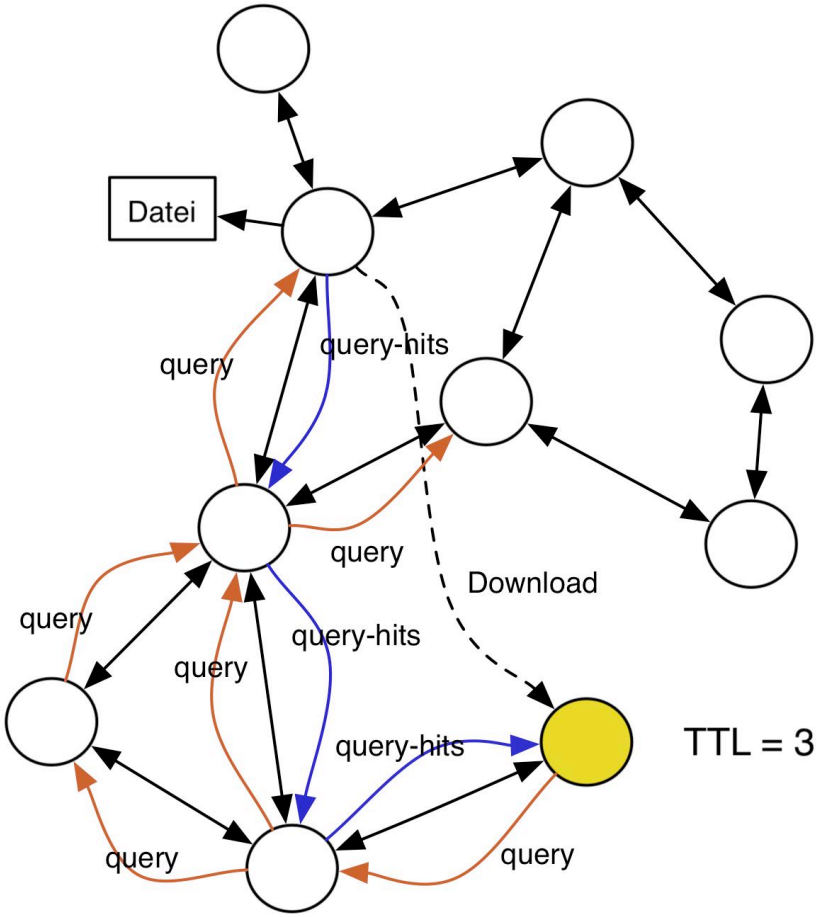
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Gnutella**
  - wurde im März 2000 herausgegeben von Justin Frankel und Tom Pepper von Nullsoft
  - Nullsoft ist seit 1999 eine Tochter von AOL
- **File-Sharing-System**
  - Ziel wie Napster
  - Arbeitet aber völlig ohne zentrale Strukturen

Beispiel Gnutella

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Dateianfrage**
  - wird an alle Nachbarn geschickt
  - diese senden sie an ihre Nachbarn
  - bis zu einer vorgegebenen Anzahl von Hops
    - TTL-Feld (time to live)
- **Protokoll**
  - **`Query`**
    - Anfrage nach Datei wird bis zu TTL-hops weitergereicht
  - **`Query-hits`**
    - Antwort auf umgekehrten Pfad
- **Wenn Datei gefunden wurde, direkter Download**



Zusammenfassung Peer-to-Peer

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Fast der gesamte Peer-to-Peer-Netzwerk-Verkehrs dient der Verletzung von Urheberrechten**
- **Aber es gibt legale Anwendungen:**
  - Internet-Telefonie, z.B. Skype
  - Software Distribution
    - zur Entlastung von Servern
  - Group Ware
    - manche Groupware-Systeme verwenden Peer-to-Peer
  - Austausch von Software unter der GNU-Lizenz
  - Austausch privater Filme, Fotos und Dokumente
- **Illegale Nutznießer von Peer-to-Peer-Netzwerken werden in letzter Zeit immer mehr gerichtlich verfolgt**

Endspurt

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Zusammenfassung der Veranstaltung**
  - „Best of“
- **Forschungsthemen in meiner Arbeitsgruppe**
  - Peer-to-Peer-Netzwerke
  - Mobile Ad-hoc-Netzwerke
  - Sensor-Netzwerke
  - Storage-Area-Netzwerke
- **Ausblick auf das nächste Semester**
  - Informatik III
  - Wireless Sensor Networks
  - Seminar Peer-to-Peer-Netzwerke

Die Schichtung des Internets - TCP/IP-Layer

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Anwendung	Application	Telnet, FTP, HTTP, SMTP (E-Mail), ...
Transport	Transport	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Vermittlung	Network	IP **(Internet Protocol)** + ICMP **(Internet Control Message Protocol)** + IGMP **(Internet Group Management Protoccol)**
Verbindung	Host-to-network	LAN **(z.B. Ethernet, Token Ring etc.)**

TCP/IP-Schichtenmodell

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

1. Host-to-Network

- nicht spezifiziert, hängt vom LAN ab

2. Vermittlungsschicht (IP - Internet Protokoll)

- Spezielles Paketformat und Protokoll
- Paketweiterleitung
- Routenermittlung

3. Transportschicht

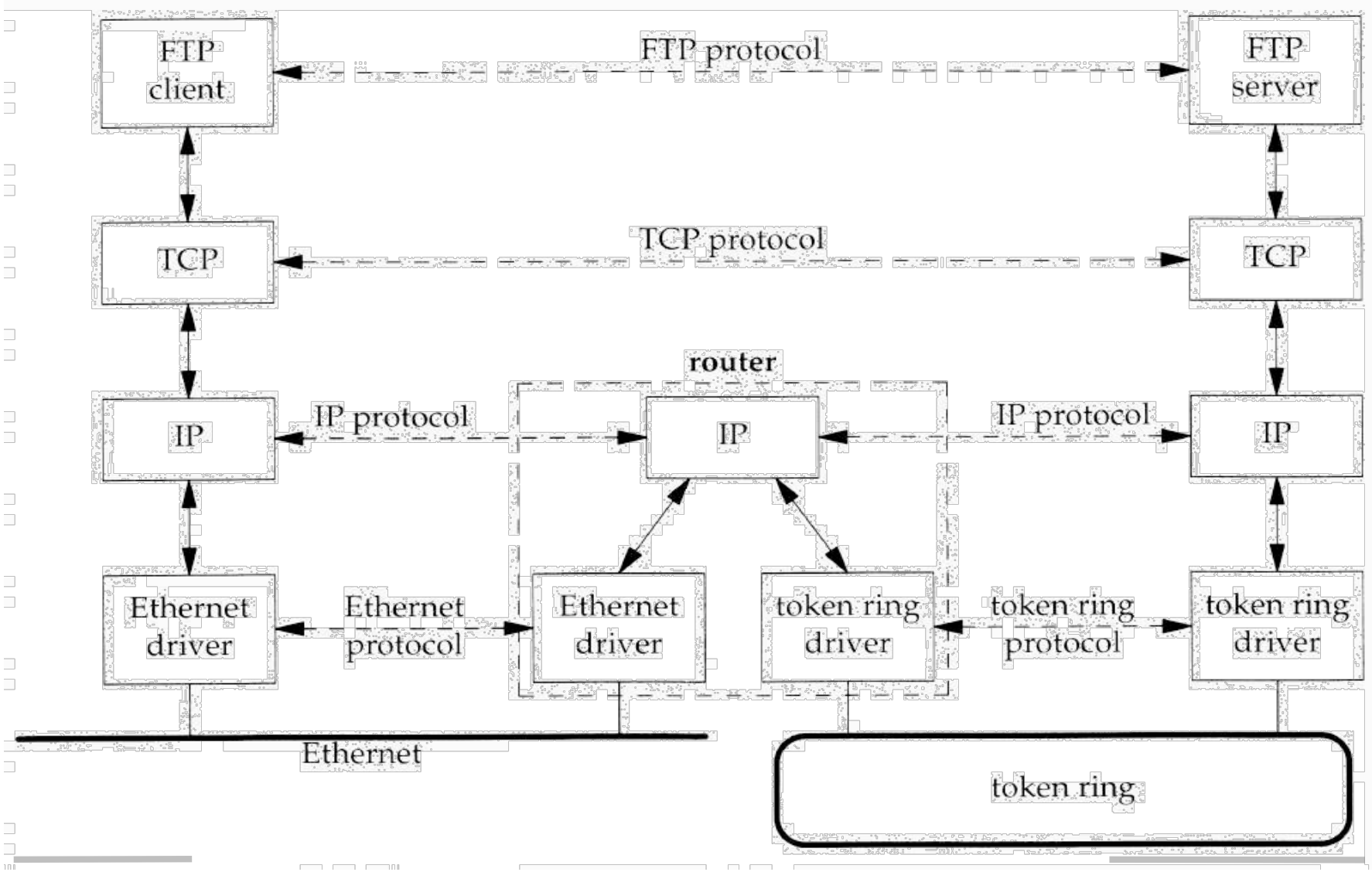
- TCP (Transport Control Protocol)
  - zuverlässiger bidirektionaler Byte-Strom-Übertragungsdienst
  - Fragmentierung, Flusskontrolle, Multiplexing
- UDP (User Datagram Protocol)
  - Paketübergabe an IP
  - unzuverlässig, keien Flusskontrolle

4. Anwendungsschicht

- zahlreiche Dienste wie TELNET, FTP, SMTP, HTTP, NNTP (für DNS), ...

Beispiel zum Zusammenspiel

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



Das ISO/OSI Referenzmodell

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

7. Anwendung (Application)
- Datenübertragung, E-Mail, Terminal, Remote login

6. Darstellung (Presentation)
- Systemabhängige Darstellung der Daten (EBCDIC/ASCII)

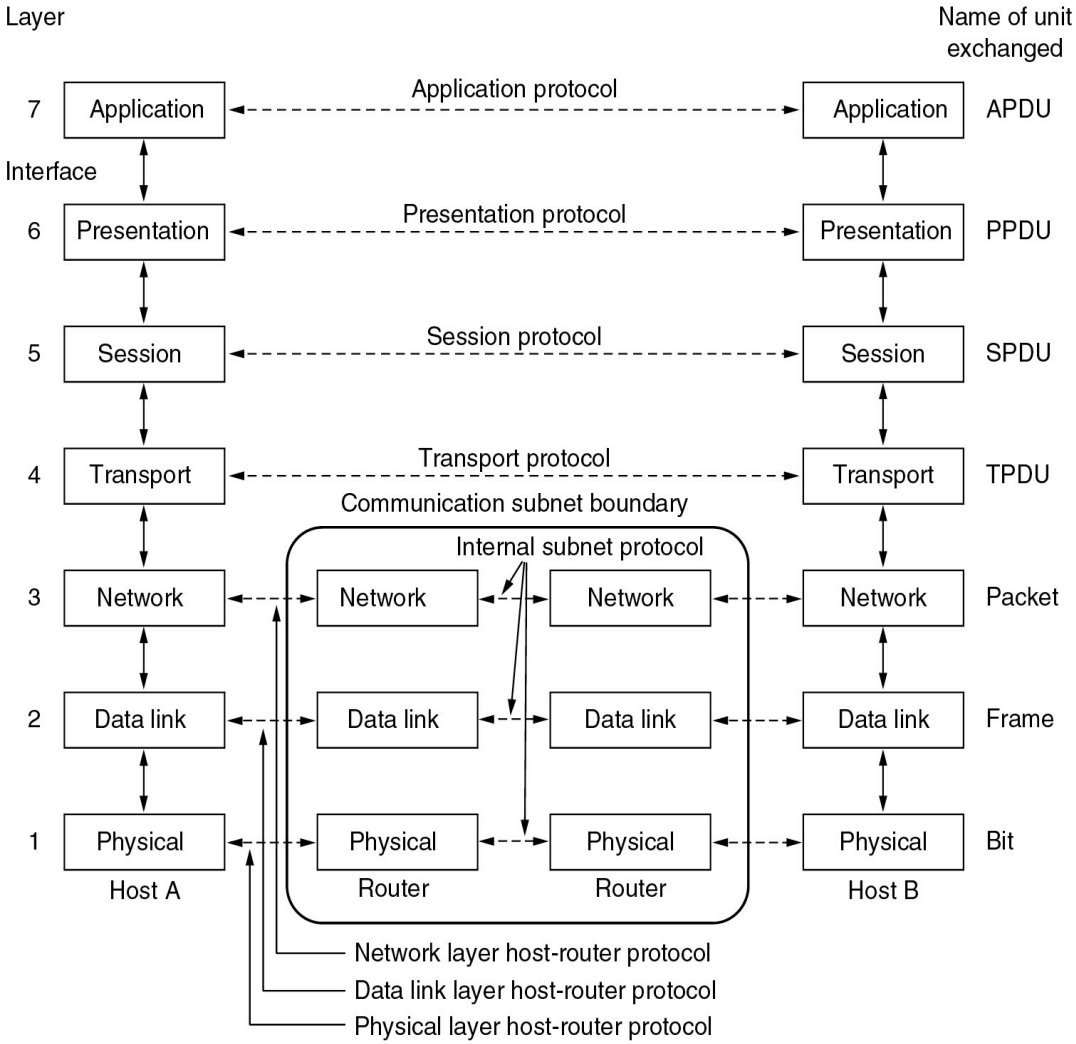
5. Sitzung (Session)
- Aufbau, Ende, Wiederaufsetzpunkte

4. Transport (Transport)
- Segmentierung, Stauvermeidung

3. Vermittlung (Network)
- Routing

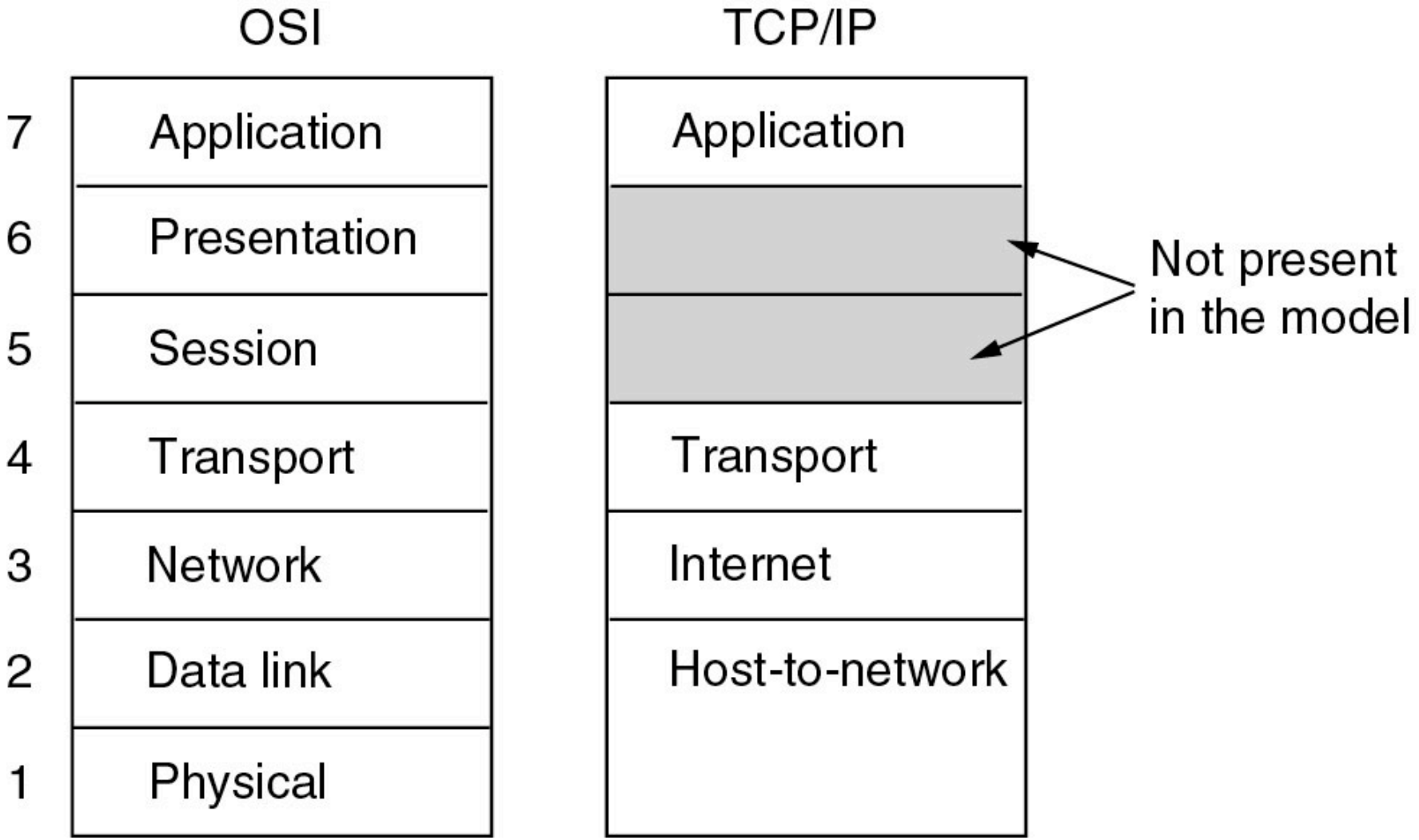
2. Sicherung (Data Link)
- Prüfsummen, Flusskontrolle

1. Bitübertragung (Physical)
- Mechanische, elektrische Hilfsmittel



OSI versus TCP/IP

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

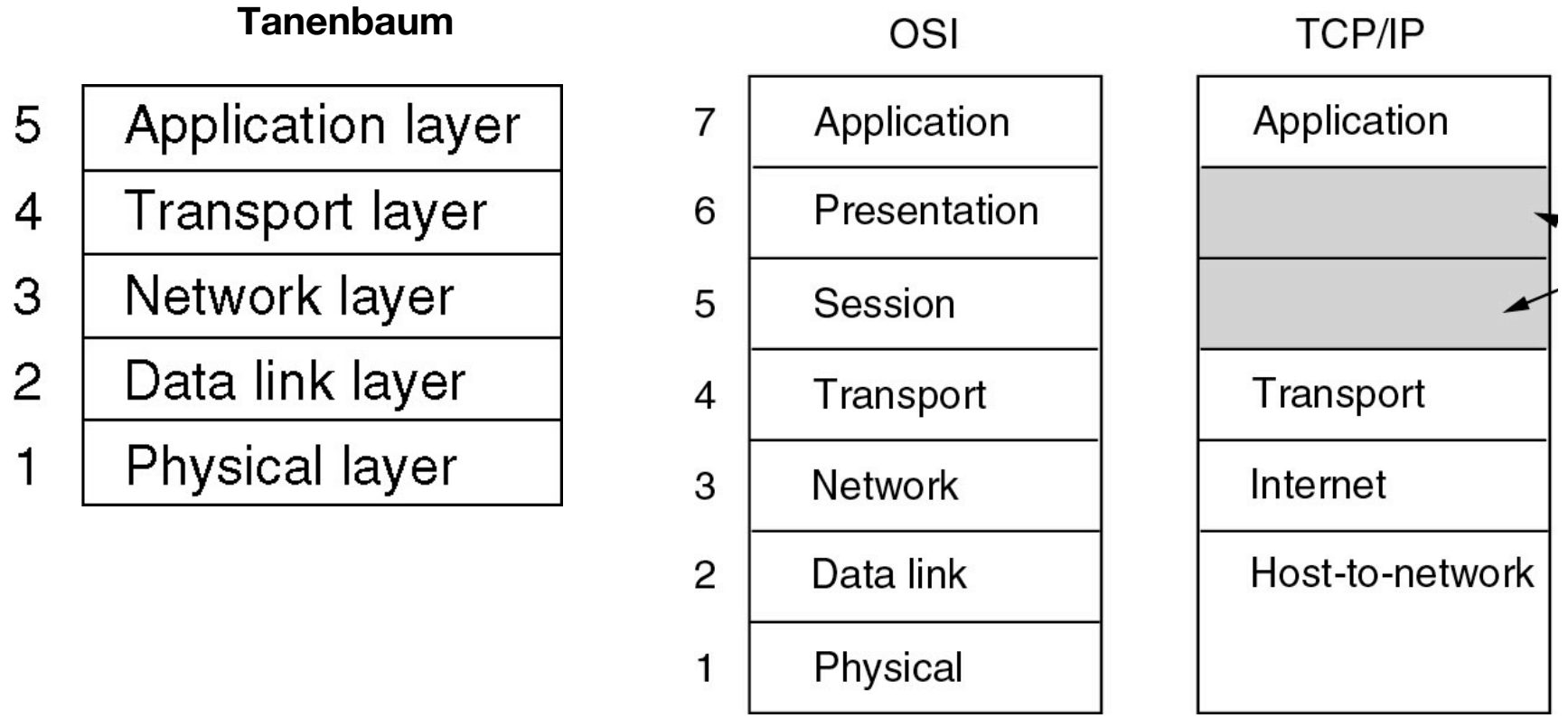


(Aus Tanenbaum)

Hybrides Modell

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Wir verwenden hier Tanenbaums hybrides Modell**



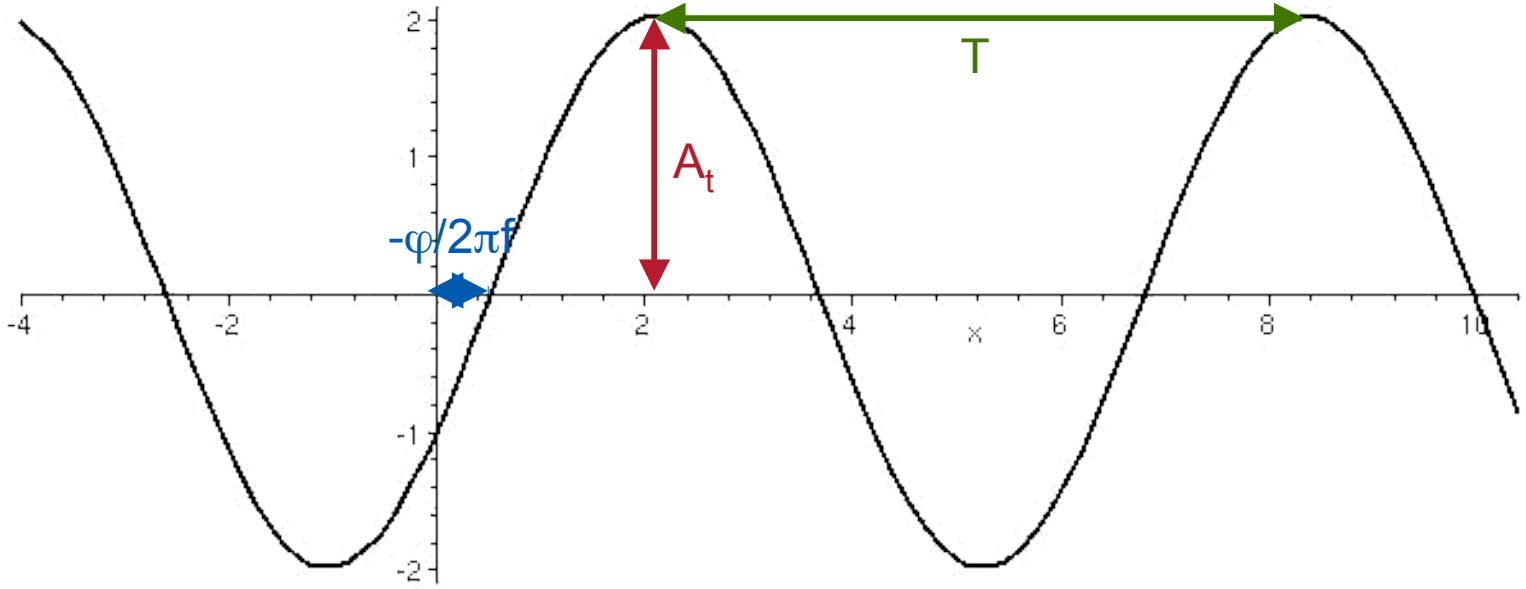
(Aus Tanenbaum)

Amplitudendarstellung

- **Amplitudendarstellung einer Sinusschwingung**

$$s(t) = A\sin(2\pi f t + \phi)$$

  - A: Amplitude — φ: Phasenverschiebung
  - f: Frequenz = 1/T — T: Periode



Fourier-Analyse für allgemeine Periode

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Der Satz von Fourier für Periode T=1/f:**
  - Die Koeffizienten *c*, a_n, b_n ergeben sich dann wie folgt

$$g(t) = \frac{a_0}{2} + \sum_{k=1}^{\infty} a_k \cos(2\pi k f t) + b_k \sin(2\pi k f t)$$

$$a_k = \frac{2}{T} \int_0^T g(t) \cos(2\pi n f t) dt$$

$$b_k = \frac{2}{T} \int_0^T g(t) \sin(2\pi n f t) dt$$

- **Die Quadratsumme der k-ten Terme ist proportional zu der Energie, die in diser Frequenz verbraucht wird:** $(a_k)^2 + (b_k)^2$
- **Üblicherweise wird die Wurzel angegeben:** $\sqrt{(a_k)^2 + (b_k)^2}$

5 Gründe für den schlechten Empfang

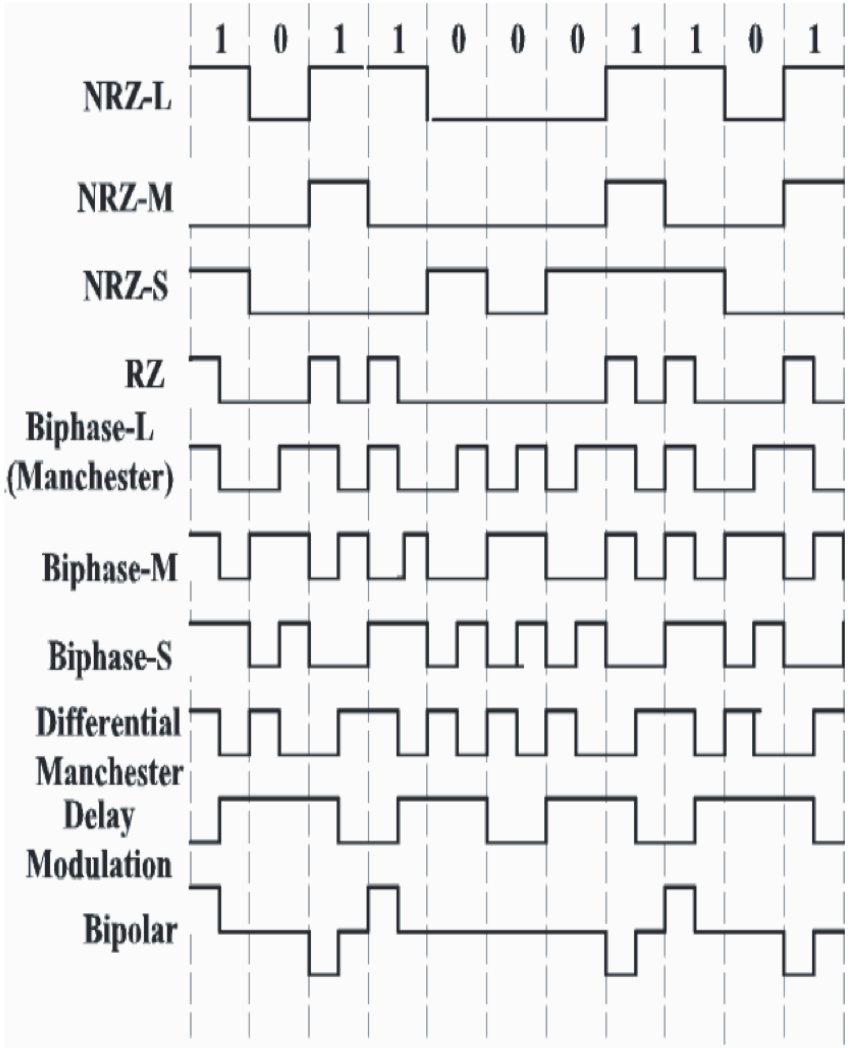
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

1. **Allgemeine Dämpfung**
2. **Frequenzverlust**
3. **Frequenzabhängige Dämpfung**
4. **Störung und Verzerrung**
5. **Rauschen**

Digitale Kodierungen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

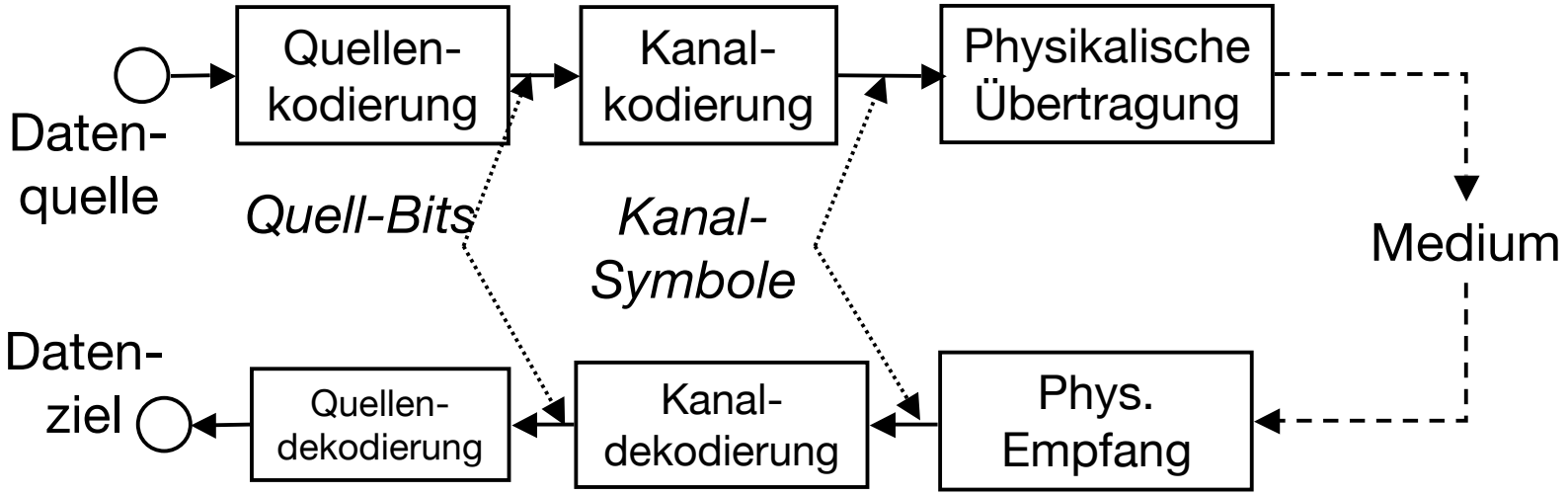
- Non-Return to Zero-Level (NRZ-L)
- Non-Return to Zero-Mark (NRZ-M)
- Non-Return to Zero-Space (NRZ-S)
- Return to Zero (RZ)
- Manchester Code (Biphase Level)
- Biphase-Mark
- Biphase-Space
- Differential Manchester-Code
- Delay Modulation (Miller)
- Bipolar



Struktur einer digitalen Basisband-Übertragung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

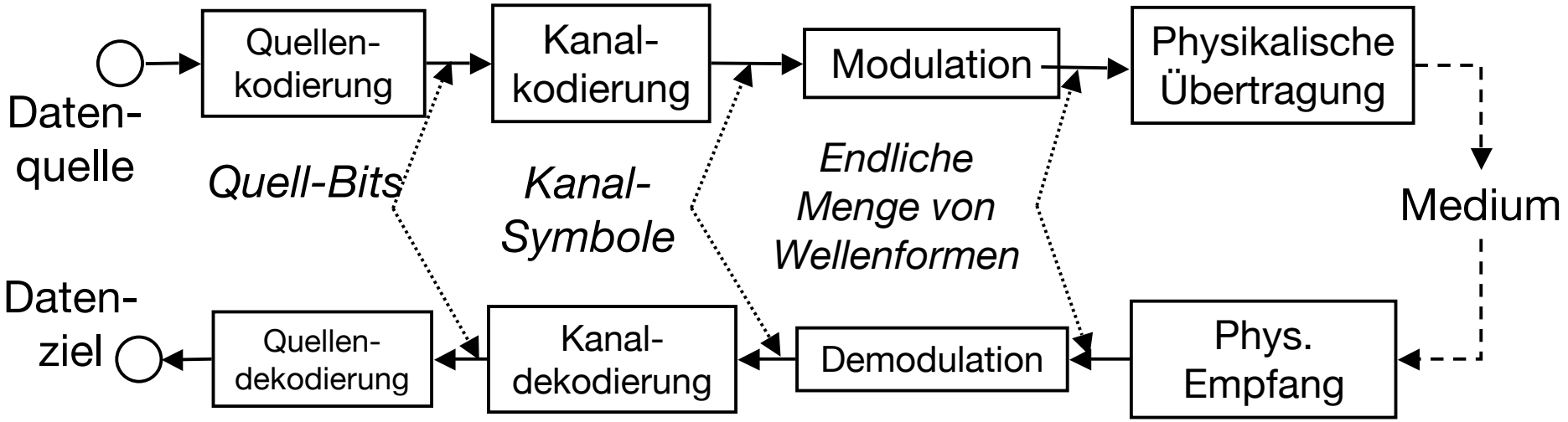
- **Quellkodierung**
  - Entfernen redundanter oder irrelevanter Information
  - Z.B. mit verlustbehafteter Komprimierung (MP3, MPEG 4)
  - oder mit verlustloser Komprimierung (Huffman-Code)
- **Kanalkodierung**
  - Abbildung der Quellbits auf Kanal-Symbole
  - Möglicherweise Hinzufügen von Redundanz angepasst auf die Kanaleigenschaften
- **Physikalische Übertragung**
  - Umwandlung in physikalische Ereignisse



Struktur einer digitalen Breitband-Übertragung

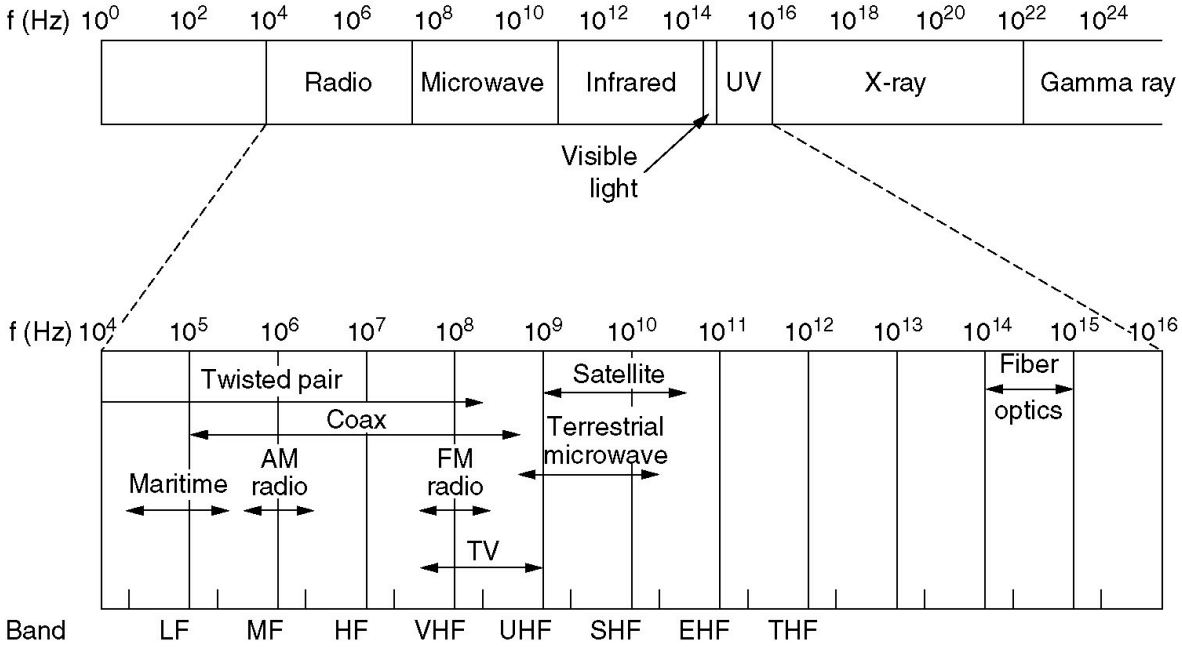
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **MOdulation/DEModulation**
  - Übersetzung der Kanalsymbole durch
    - Amplitudenmodulation
    - Phasenmodulation
    - Frequenzmodulation
    - oder einer Kombination davon



Frequenzbereiche

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



LF Low Frequency =
LW Langwelle

MF Medium Frequency =
MW Mittelwelle

HF High Frequency =
KW Kurzwelle

VHF Very High Frequency =
UKW Ultrakurzwelle

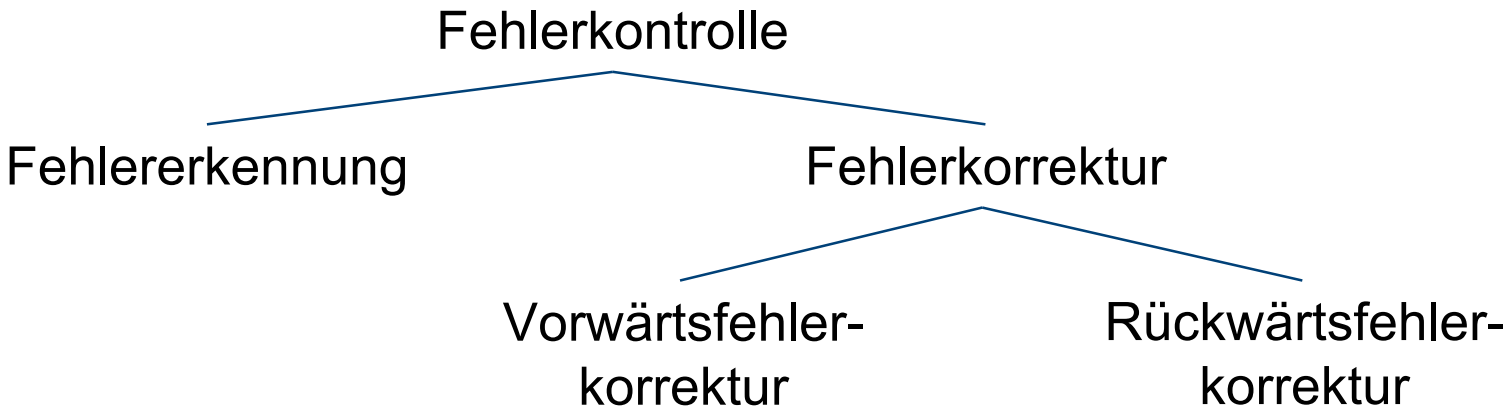
UHF Ultra High Frequency
SHF Super High Frequency
EHF Extra High Frequency

UV Ultraviolettes Licht
X-ray Röntgenstrahlung

Fehlerkontrolle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

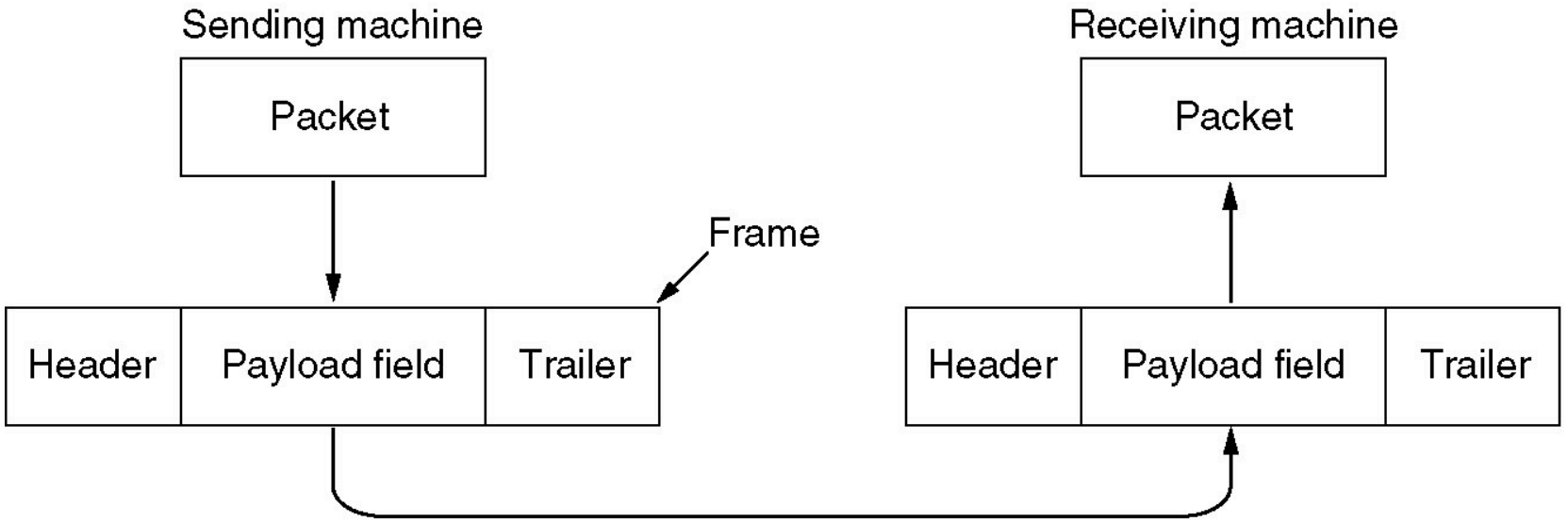
- **Zumeist gefordert von der Vermittlungsschicht**
  - Mit Hilfe der Frames
- **Fehlererkennung**
  - Gibt es fehlerhaft übertragene Bits
- **Fehlerkorrektur**
  - Behebung von Bitfehlern
  - Vorwärtsfehlerkorrektur (Forward Error Correction)
    - Verwendung von redundanter Kodierung, die es ermöglicht Fehler ohne zusätzliche Übertragungen zu beheben
  - Rückwärtsfehlerkorretur (Backward Error Correction)
    - Nach Erkennen eines Fehlers, wird durch weitere Kommunikation der Fehler behoben



Header und Trailer

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Header und Trailer**
  - Zumeist verwendet man **Header** am Anfang des Frames, mitunter auch **Trailer** am Ende des Frames
  - signalisieren den Frame-Beginn und Frame-Ende
  - tragen Kontrollinformationen
    - z.B. Sender, Empfänger, Frametypen, Fehlerkontrollinformation

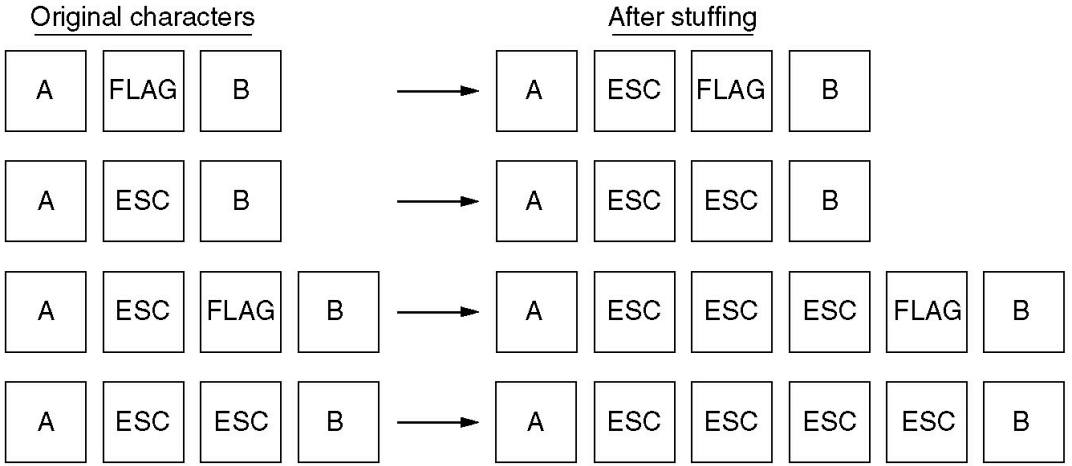


Flag Bytes und Bytestopfen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Besondere "Flag Bytes" markieren Anfang und Ende eines Frames**

- **Falls diese Marker in den Nutzdaten vorkommen**
  - Als Nutzdatenbyte mit Sonderzeichen (Escape) markieren
    - Bytestopfen (byte stuffing)
  - Falls Sonderzeichen und "Flag-Byte" erscheinen, dito,
    - etc. ,etc.



Hamming Distanz

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Der "Abstand" der erlaubten Nachrichten zueinander war immer als zwei Bits**
- **Definition: Hamming-Distanz**

  Seien $x=x_1,\ldots, x_n$ und $y=y_1,\ldots, y_n$ Nachrichten

  Dann sei d(x,y) = die Anzahl der 1er Bits in x XOR y
- **Intuitiver: die Anzahl der Positionen, in denen sich x und y unterscheiden**
- **Die Hamming-Distanz ist eine Metrik**
  - Symmetrie, Dreiecksungleichung

Beispiel:

x=0011010111
y=0110100101
x XOR y=0101110010

d(x,y) = 5

Hamming-Distanz von Nachrichtenmengen

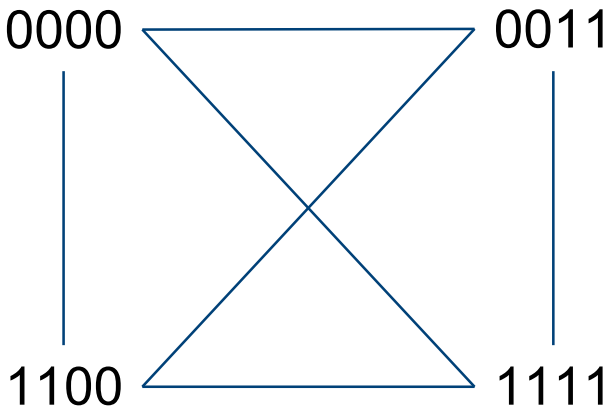
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

➢ **Die Hamming-Distanz einer Menge von (gleich langen) Bit-Strings S ist:**

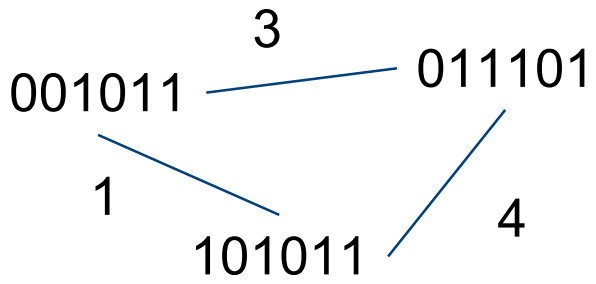
$$d(S) = \min_{x,y \in S, x \neq y} d(x,y)$$

– d.h. der kleinste Abstand zweier verschiedener Worte in S

Beispiel:



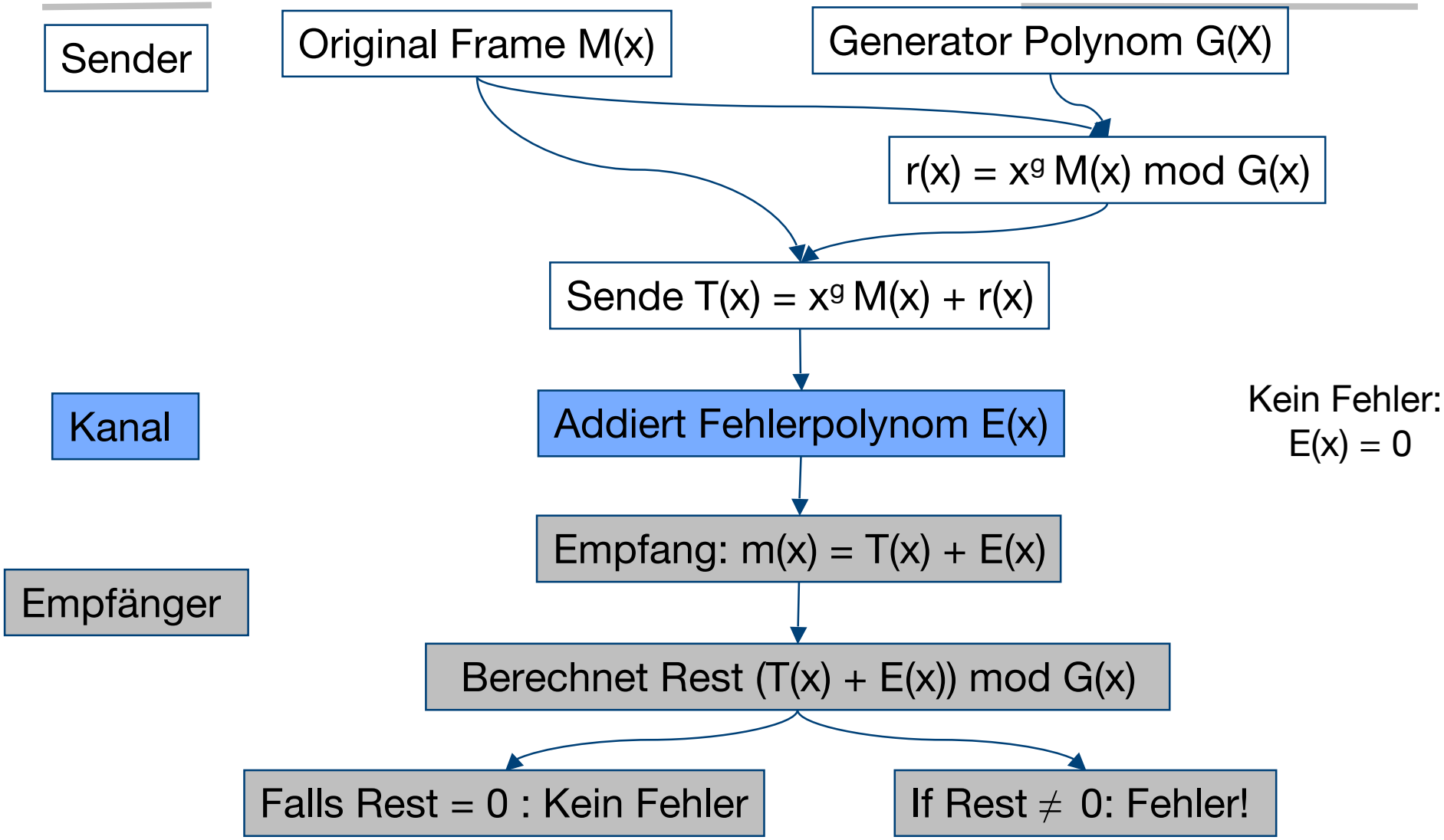
Alle Abstände sind 2



Ein Abstand ist 1!

CRC – Überblick

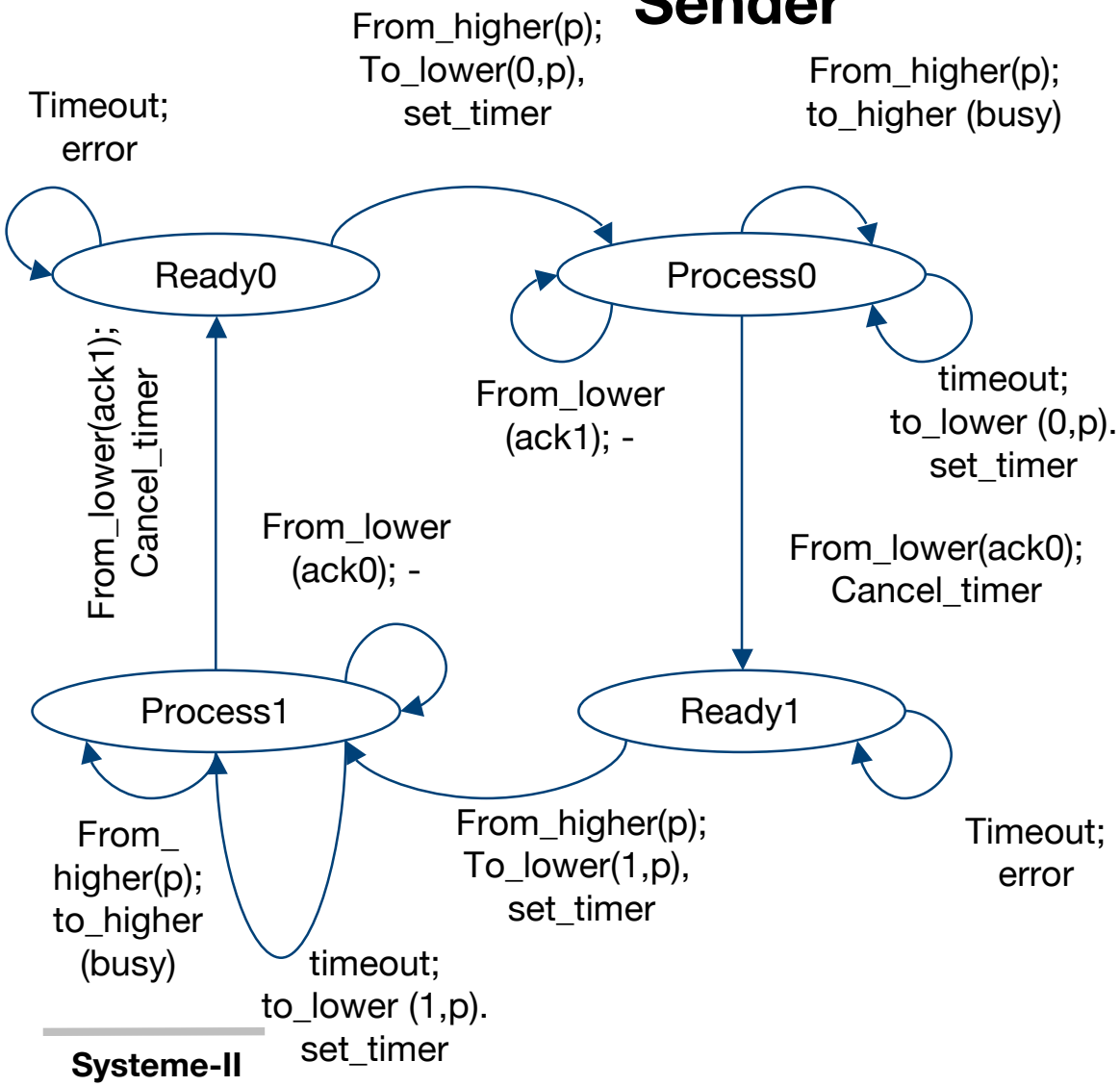
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



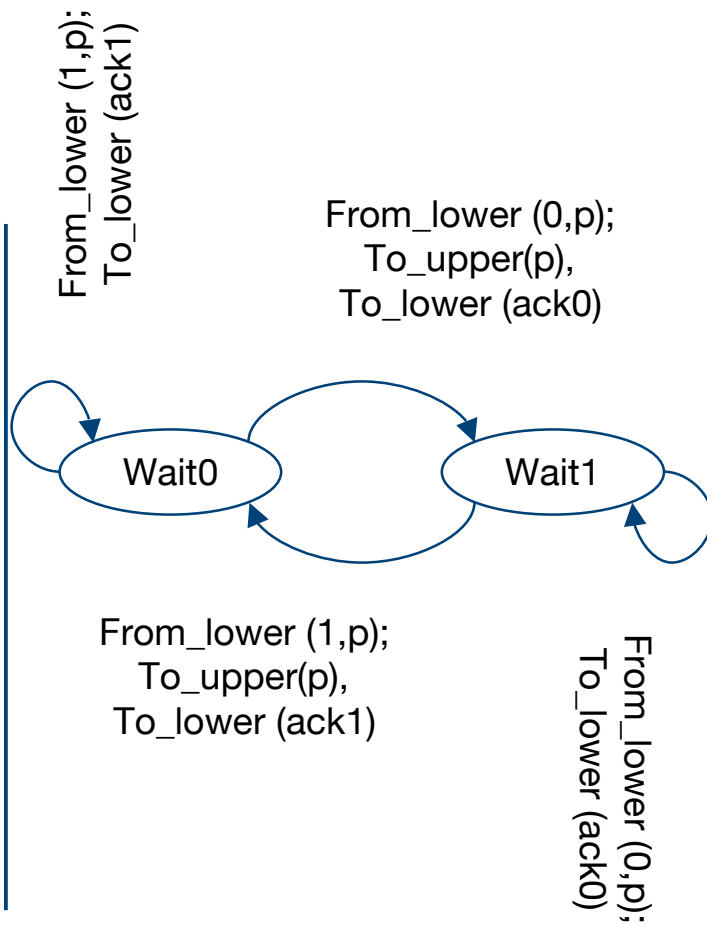
3. Versuch: Bestätigung und Sequenznummern

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Sender



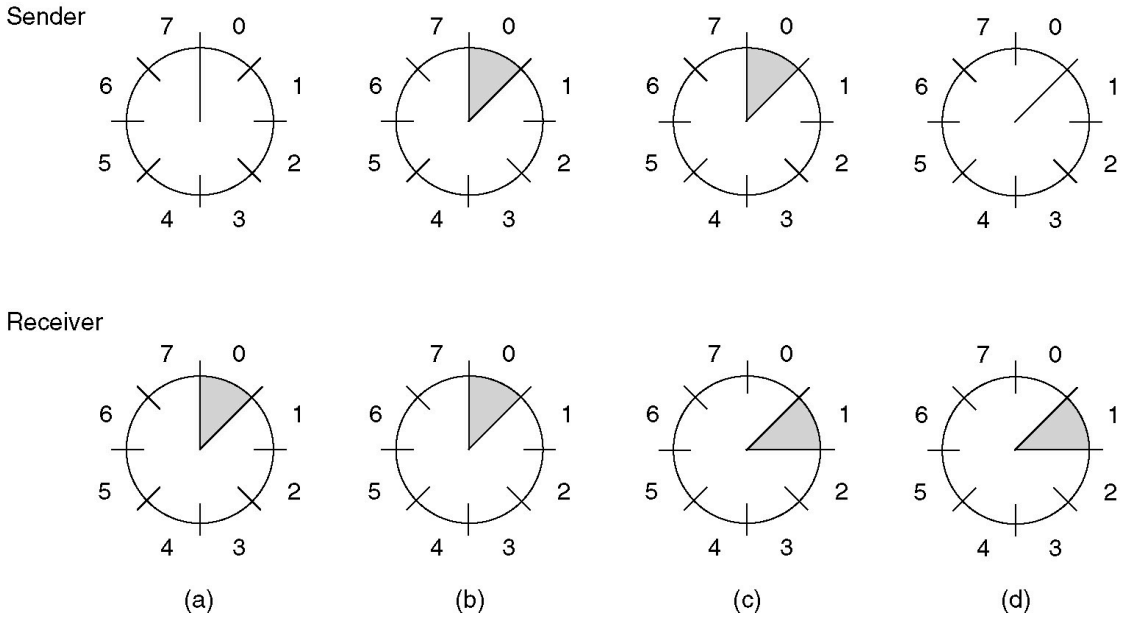
Empfänger



Beispiel

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **“Sliding Window”-Beispiel für n=3 und fester Fenstergröße = 1**
- **Der Sender zeigt die momentan unbestätigten Sequenznummern an**
  - Falls die maximale Anzahl nicht bestätigter Frames bekannt ist, dann ist das das Sende-Fenster



a. Initial: Nichts versendet

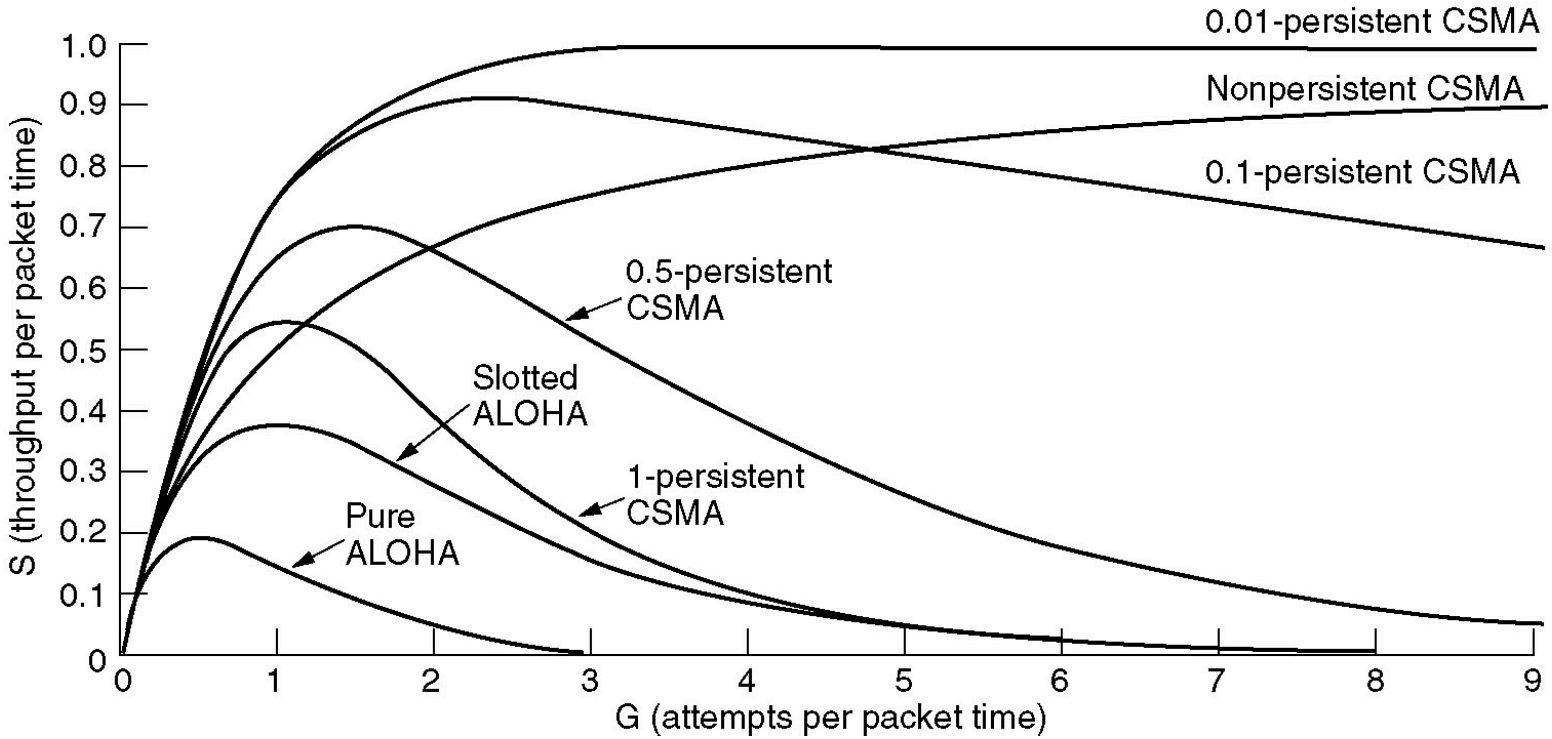
b. Nach Senden des 1. Frames mit Seq.Nr. 0

c. Nach dem Empfang des 1. Frame

d. Nach dem Empfang der Bestätigung

Effizienz von CSMA

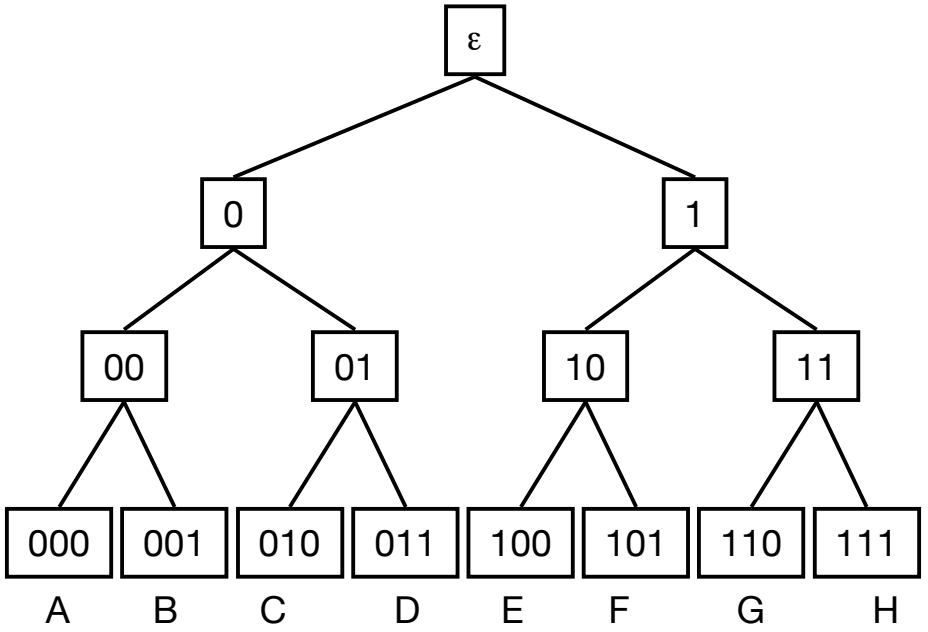
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

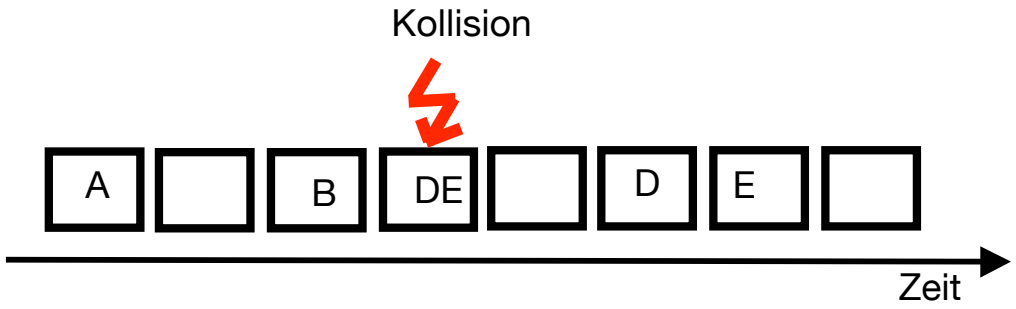


Adaptives Baumprotokoll Voraussetzung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Adaptives Baumprotokoll (adaptive tree walk)**
- **Ausgangspunkt:**
  - Binäre, eindeutige Präsentation aller Knoten (ID)
  - Dargestellt in einem Baum
  - Synchronisiertes Protokoll
  - Drei Typen können unterschieden werden:
    - Keine Station sendet
    - Genau eine Station sendet
    - Kollision: mindestens zwei Stationen senden





Kürzeste Wege mit Edsger Wybe Dijkstra

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Dijkstra(G, w, s)
begin
    Init-Single-Source(G, w)
    $S \leftarrow \emptyset$
    $Q \leftarrow V$
    while $Q \neq \emptyset$ do
        $u \leftarrow$ Element aus Q mit minimalen Wert $d(u)$
        $S \leftarrow S \cup \{u\}$
        $Q \leftarrow Q \setminus \{u\}$
        for all $v \in$ Adj(u) do
            Relax(u, v)
        od
    od
end

Dijkstras Kürzeste-Wege-Algorithmus kann mit Laufzeit Θ(|E| + |V| log |V|) implementiert werden.

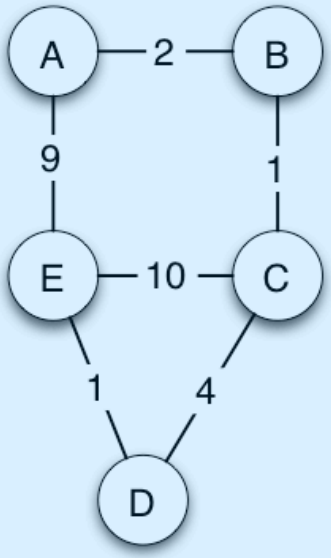
Init-Single-Source(G, w, s)
begin
    for all $v \in V$ do
        $d(v) \leftarrow \infty$
        $\pi(v) \leftarrow v$
    od
    $d(s) \leftarrow 0$
end

Relax(u, v)
begin
    if $d(v) > d(u) + w(u, v)$ then
        $d(v) \leftarrow d(u) + w(u, v)$
        $\pi(v) \leftarrow u$
    fi
end

Distance Vector Routing Protocol

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Distance Table Datenstruktur**
  - Jeder Knoten besitzt eine
    - Zeile für jedes mögliches Ziel
    - Spalte für jeden direkten Nachbarn
- **Verteilter Algorithmus**
  - Jeder Knoten kommuniziert nur mit seinem Nachbarn
- **Asynchroner Betrieb**
  - Knoten müssen nicht Informationen austauschen in einer Runde
- **Selbstterminierend**
  - läuft bis die Knoten keine Information mehr austauschen



Distance Table für A

	von A	über B	über E	Routing Tabellen Eintrag
nach	B	2	15	B
	C	3	14	B
	D	7	10	B
	E	13	9	E

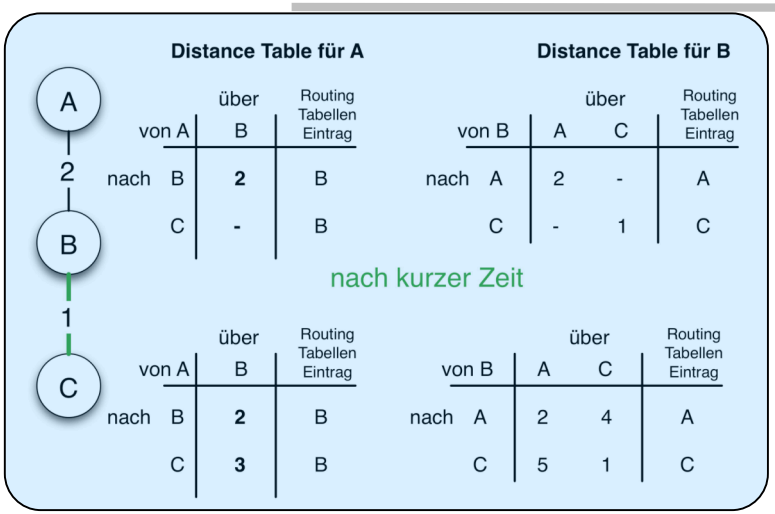
Distance Table für C

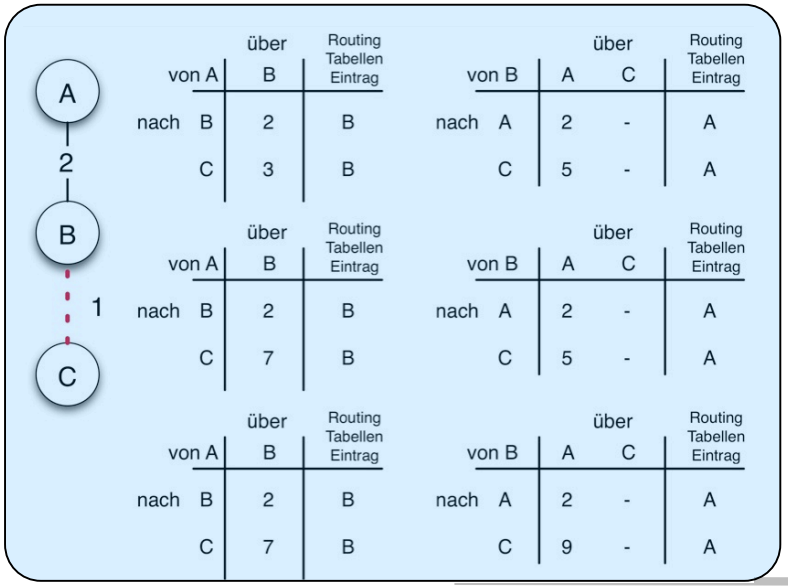
	von C	über B	über D	über E	Routing Tabellen Eintrag
nach	A	3	11	18	B
	B	1	6	16	B
	D	5	4	11	D
	E	7	5	10	D

Das “Count to Infinity” - Problem

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Gute Nachrichten verbreiten sich schnell**
  - Neue Verbindung wird schnell veröffentlicht
- **Schlechte Nachrichten verbreiten sich langsam**
  - Verbindung fällt aus
  - Nachbarn erhöhen wechselseitig ihre Entfernung
  - “Count to Infinity”-Problem

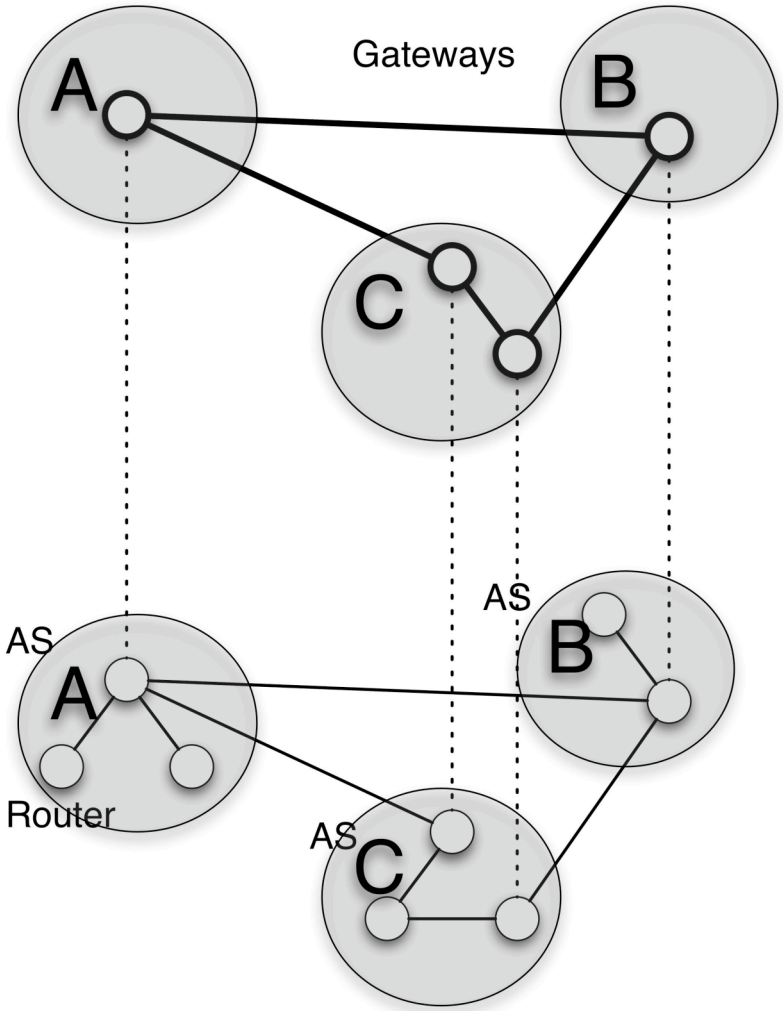




AS, Intra-AS und Inter-AS

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Autonomous System (AS)**
  - liefert ein zwei Schichten-Modell des Routing im Internet
  - Beispiele für AS:
    - uni-paderborn.de
- **Intra-AS-Routing (Interior Gateway Protocol)**
  - ist Routing innerhalb der AS
  - z.B. RIP, OSPF, IGRP, ...
- **Inter-AS-Routing (Exterior Gateway Protocol)**
  - Übergabepunkte sind Gateways
  - ist vollkommen dezentrales Routing
  - Jeder kann seine Optimierungskriterien vorgeben
  - z.B. EGP (früher), BGP



Transportschicht (transport layer)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **TCP (transmission control protocol)**
  - Erzeugt zuverlässigen Datenfluß zwischen zwei Rechnern
  - Unterteilt Datenströme aus Anwendungsschicht in Pakete
  - Gegenseite schickt Empfangsbestätigungen (Acknowledgments)
- **UDP (user datagram protocol)**
  - Einfacher unzuverlässiger Dienst zum Versand von einzelnen Päckchen
  - Wandelt Eingabe in ein Datagramm um
  - Anwendungsschicht bestimmt Paketgröße
- **Versand durch Netzwerkschicht**
- **Kein Routing: End-to-End-Protokolle**

TCP - Algorithmus von Nagle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Wie kann man sicherstellen,**
  - dass kleine Pakete zeitnah ausgeliefert werden
  - und bei vielen Daten große Pakete bevorzugt werden?

- **Algorithmus von Nagle:**
  - Kleine Pakete werden nicht versendet, solange Bestätigungen noch ausstehen.
    - Paket ist klein, wenn Datenlänge < MSS
  - Trifft die Bestätigung des zuvor gesendeten Pakets ein, so wird das nächste verschickt.
- **Beispiel:**
  - Telnet versus ftp
- **Eigenschaften**
  - Selbst-taktend: Schnelle Verbindung = viele kleine Pakete

Stauvermeidung in TCP Tahoe

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

x: Anzahl Pakete pro RTT

- **Jacobson 88:**
  - Parameter: cwnd und Slow-Start-Schwellwert (ssthresh=slow start threshold)
  - S = Datensegmentgröße = maximale Segmentgröße
- **Verbindungsaufbau:**
  cwnd ← S **ssthresh ← 65535**

  x ← 1
  y ← max
- **Bei Paketverlust, d.h. Bestätigungsdauer > RTO,**
  - multiplicatively decreasing
    cwnd ← S ssthresh ← $\max\left\{2{\times}S, \frac{\min\{cwnd, wnd\}}{2}\right\}$

    x ← 1
    y ← x/2
- **Werden Segmente bestätigt und cwnd ≤ ssthresh, dann**
  - slow start:
    cwnd ← cwnd + S

    x ← 2·x, bis x = y
- **Werden Segmente bestätigt und cwnd > ssthresh, dann additively increasing**
  cwnd ← cwnd + S $\frac{S}{cwnd}$

  x ← x +1

TCP Tahoe

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

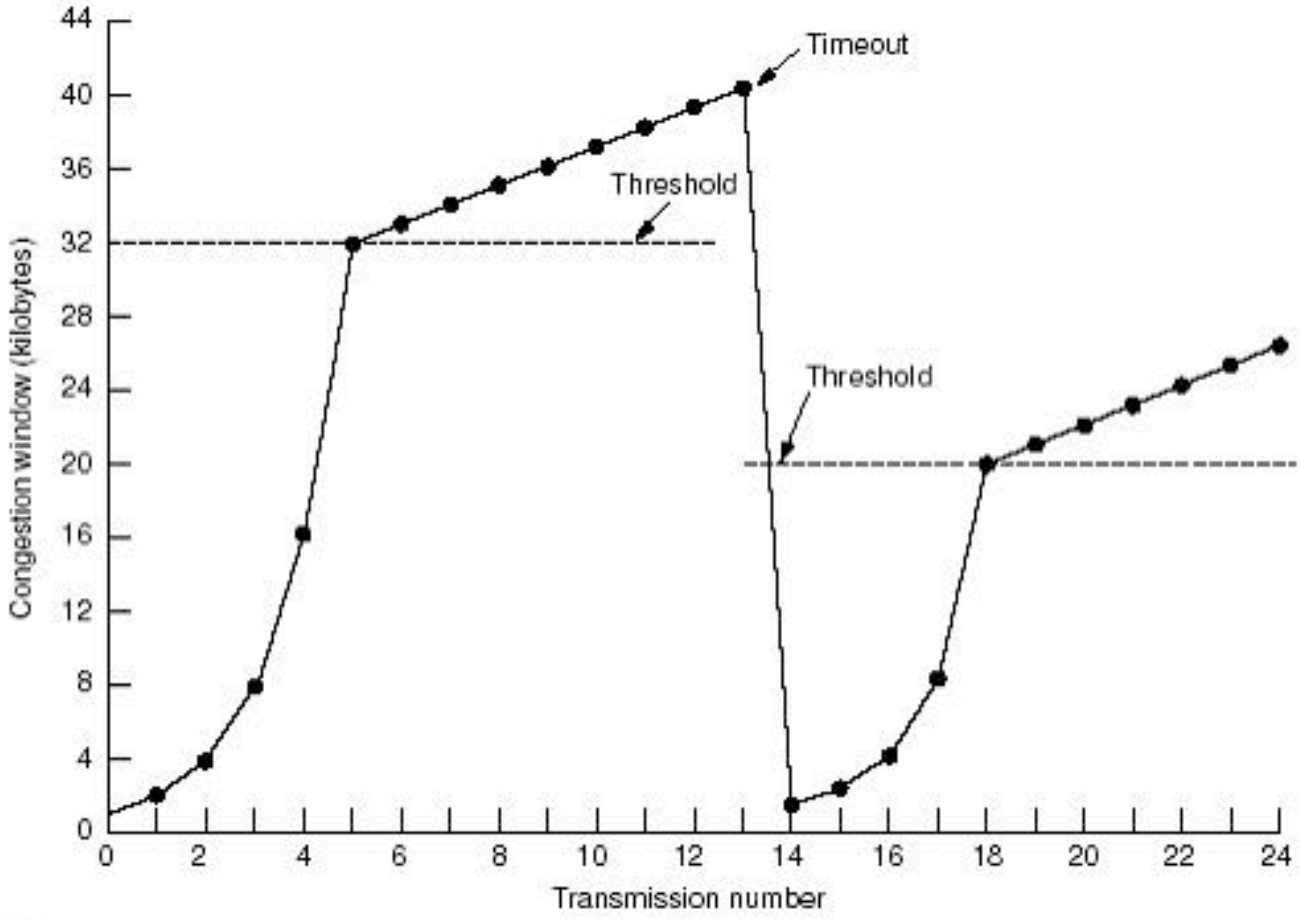
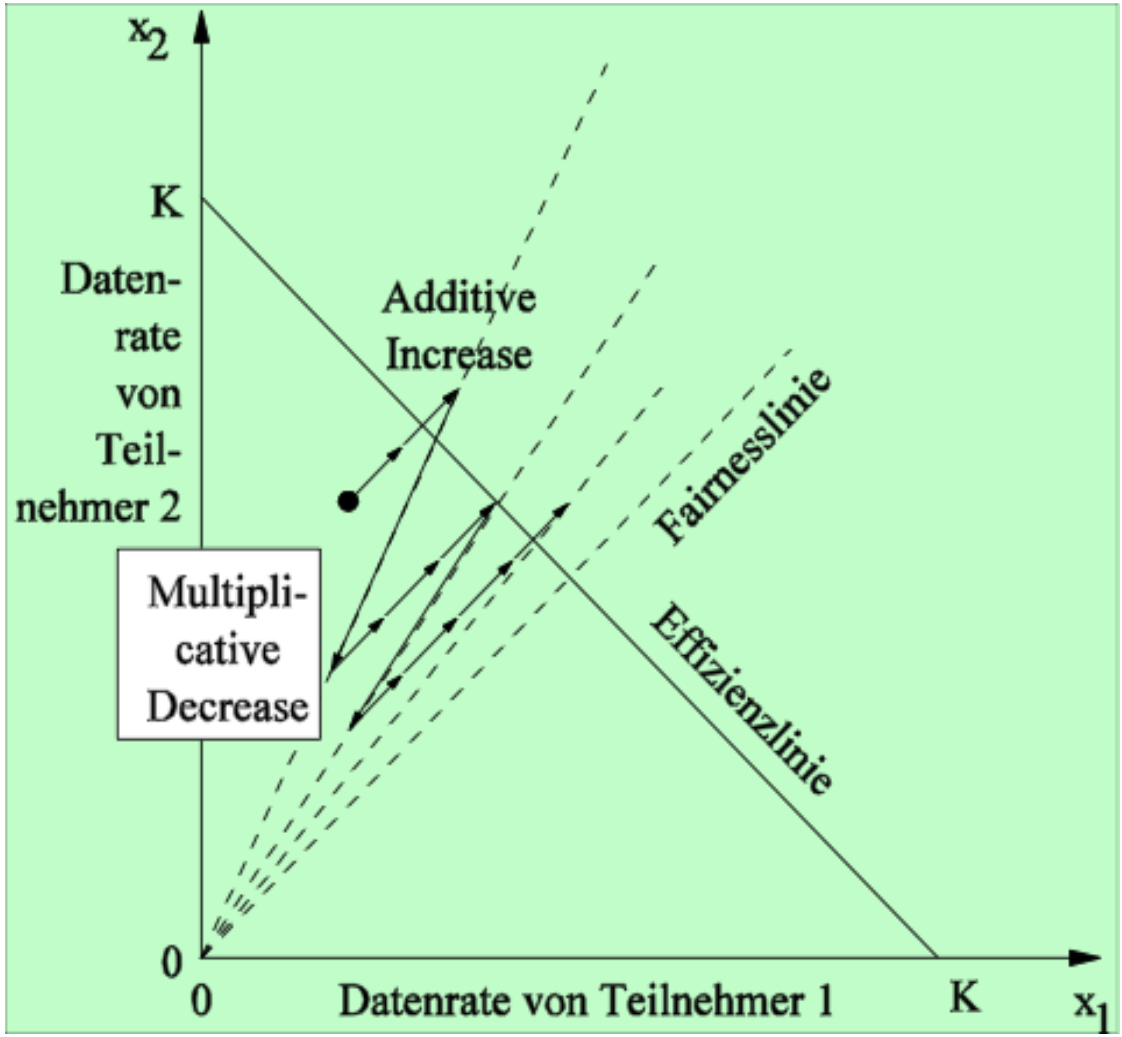


Fig3

pictures from TANENBAUM A. S. *Computer Networks 3rd edition*

AIMD: Additively Increase/ Multiplicatively Decrease

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



Bedrohungen und Sicherheitsziele

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Verschlüsselungs-methoden

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Symmetrische Verschlüsselungsverfahren**
  - z.B. Cäsars Code
  - Enigma
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- **Kryptografische Hash-Funktion**
  - SHA-1, SHA-2, MD5
- **Asymmetrische Verschlüsselungsverfahren**
  - RSA (Rivest, Shamir, Adleman)
  - Diffie-Helman
- **Digitale Unterschriften (Elektronische Signature)**
  - PGP (Phil Zimmermann), RSA

Firewalls

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

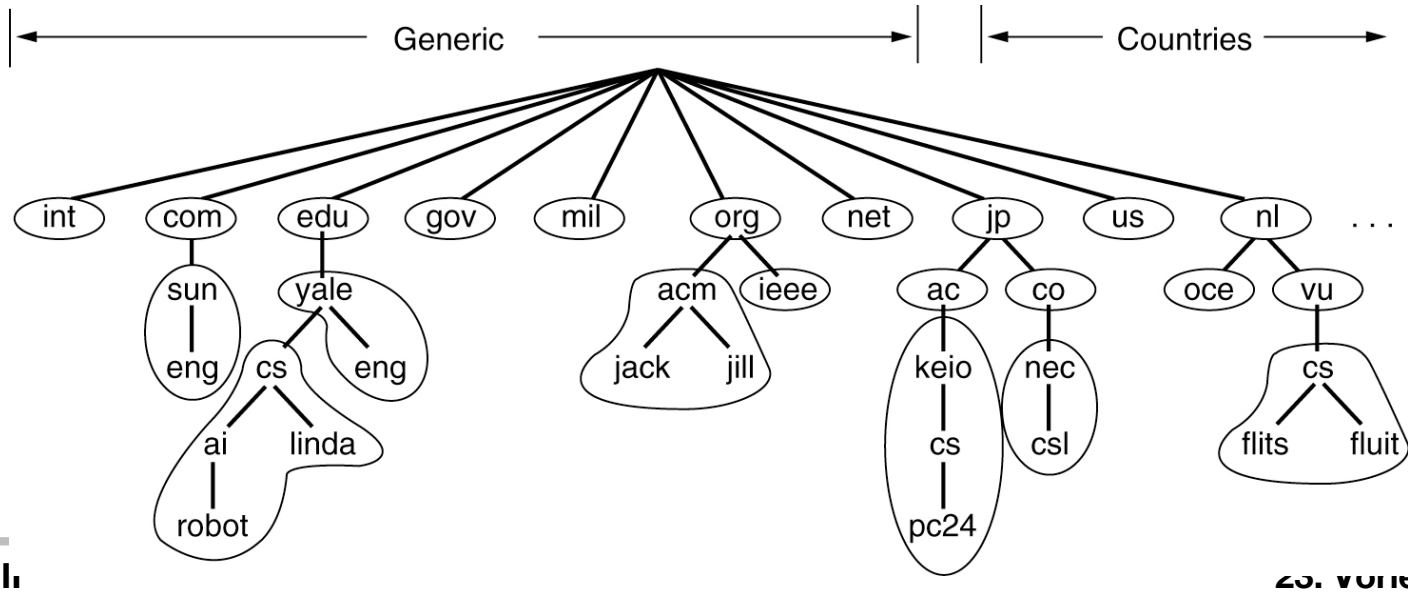
- **Typen von Firewalls**
  - Host-Firewall
  - Netzwerk-Firewall
- **Netzwerk-Firewall**
  - unterscheidet
    - Externes Netz (Internet-feindselig)
    - Internes Netz (LAN-vertrauenswürdig)
    - Demilitarisierte Zone (vom externen Netz erreichbare Server)
- **Host-Firewall**
  - z.B. Personal Firewall
  - kontrolliert den gesamten Datenverkehr eines Rechners
  - Schutz vor Attacken von außerhalb und von innen (Trojanern)

- **Methoden**
  - Paketfilter
    - Sperren von Ports oder IP-Adressen
  - Content-Filter
    - Filtern von SPAM-Mails, Viren, ActiveX oder JavaScript aus HTML-Seiten
  - Proxy
    - Transparente (extern sichtbare) Hosts
    - Kanalisierung der Kommunikation und möglicher Attacken auf gesicherte Rechner
  - NAT, PAT
    - Network Address Translation
  - Bastion Host
  - Proxy

DNS Name Server

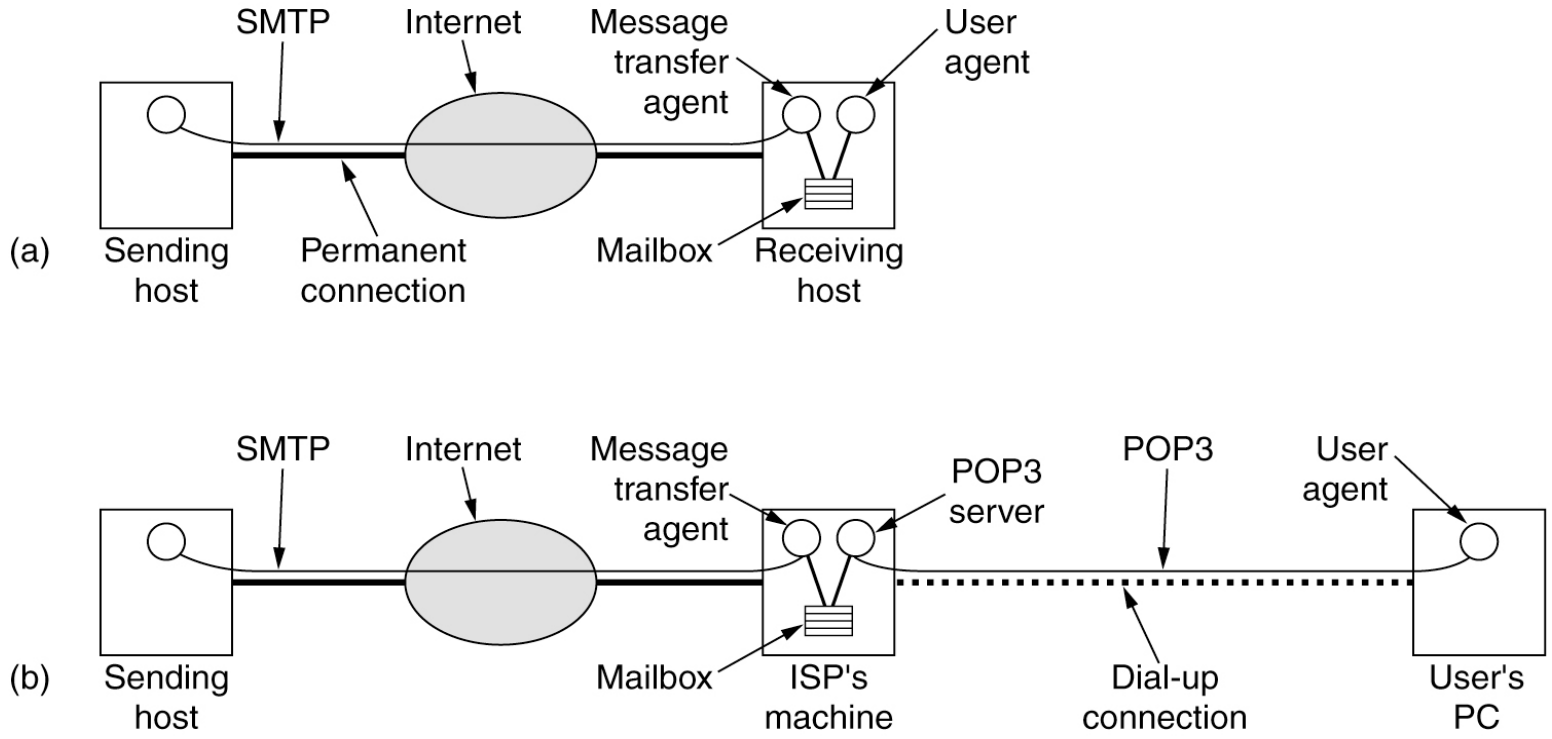
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Der Namensraum ist in Zonen aufgeteilt**
- **Jede Zone hat einen *Primary Name Server* mit maßgeblicher Information**
  - Zusätzlich **Secondary Name Server** für Zuverlässigkeit
- **Jeder Name Server kennt**
  - seine eigene Zone
  - Name-Server der darunterliegenden Bereiche
  - Bruder-Name-Server oder zumindestens einen Server, der diese kennt



E-Mail: SMTP und POP

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



SMTP: Simple Mail Transfer Protocol
POP: Post Office Protocol
IMAP: Internet Message Access Protocol

Ende der 23. Vorlesung

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Systeme II

Christian Schindelhauer

schindel@informatik.uni-freiburg.de