

*Advanced computer networking*

# Internet Protocols

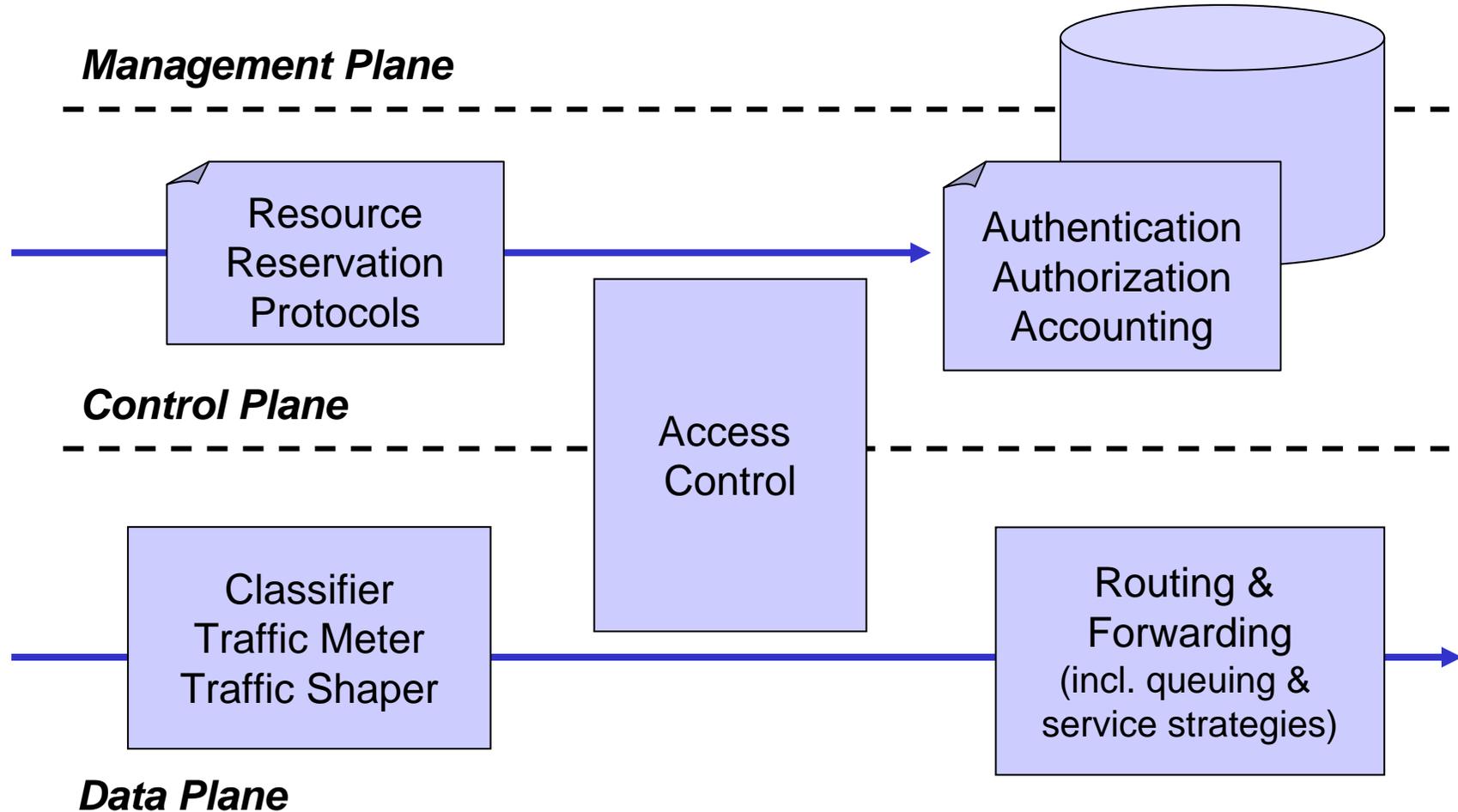
---

*Thomas Fuhrmann*



Network Architectures  
Computer Science Department  
Technical University Munich

# The QoS Landscape



Es gab bereits mehrere Ansätze für Dienstgüte im Internet:

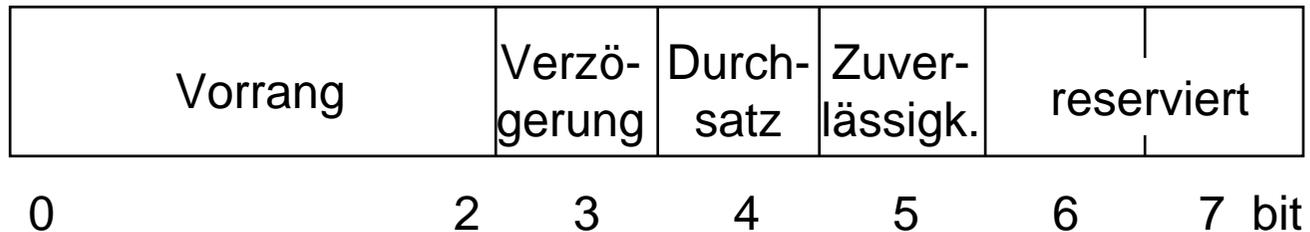
- IP *Type of Service*, hat sich nicht durchgesetzt
- *Stream Transport Protocol Version 2+* (ST2+):
  - Hard-State für Reservierungsinformation, eigenes Protokoll neben IP
  - Nicht in der Praxis eingesetzt, nur noch von historischem Interesse
- *Integrated Services*
  - Drei festgelegte Dienste: Guaranteed Service, Controlled Load, Best-Effort
  - Empfängerorientiertes Signalisierungsprotokoll RSVP
  - Soft-State für Reservierungsinformation
  - Zu aufwendig für die Praxis, hat sich nicht durchgesetzt
- *Differentiated Services*
  - Unterstützung für max. 64 verschiedene Dienstklassen
  - Implizite Signalisierung der Dienstklasse in der Dateneinheit
  - Aggregation von Verkehr reduziert Aufwand im Netzinneren
  - Hat sich (noch) nicht durchgesetzt ...

# Type of Service-Feld

Dienstqualität in IP-Datagrammen ursprünglich durch Type-of-Service (ToS) vorgesehen (RFC 791):

- Vorrang: verschiedene Prioritätsstufen
- Verzögerung: normale (0), niedrig (1)
- Durchsatz: normal (0), hoch (1)
- Zuverlässigkeit: normal (0), hoch (1)

Mit dem ToS-Feld alleine können keine Garantien gegeben werden.



RFC 791: "The use of the Delay, Throughput and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another."

Architektur für Integrierte Dienste (Mitte der 90er Jahre):

- Unterstützung multimedialer Anwendungen (z.B. Video-Konferenzen)
- Abkehr vom zustandslosen Router:
  - Zustand pro Datenstrom in jedem Router
  - Behandlung der Pakete wie im Verkehrsprofil angegeben
  - „Soft State“-Reservierung (statt „No-State“ im klassischen Internet)
- Ergänzung der bestehenden Internet-Architektur
- Integration gruppenkommunikationsbasierter Anwendungen
- Ressourcen-Reservierungen über das Resource Reservation Protocol (RSVP)

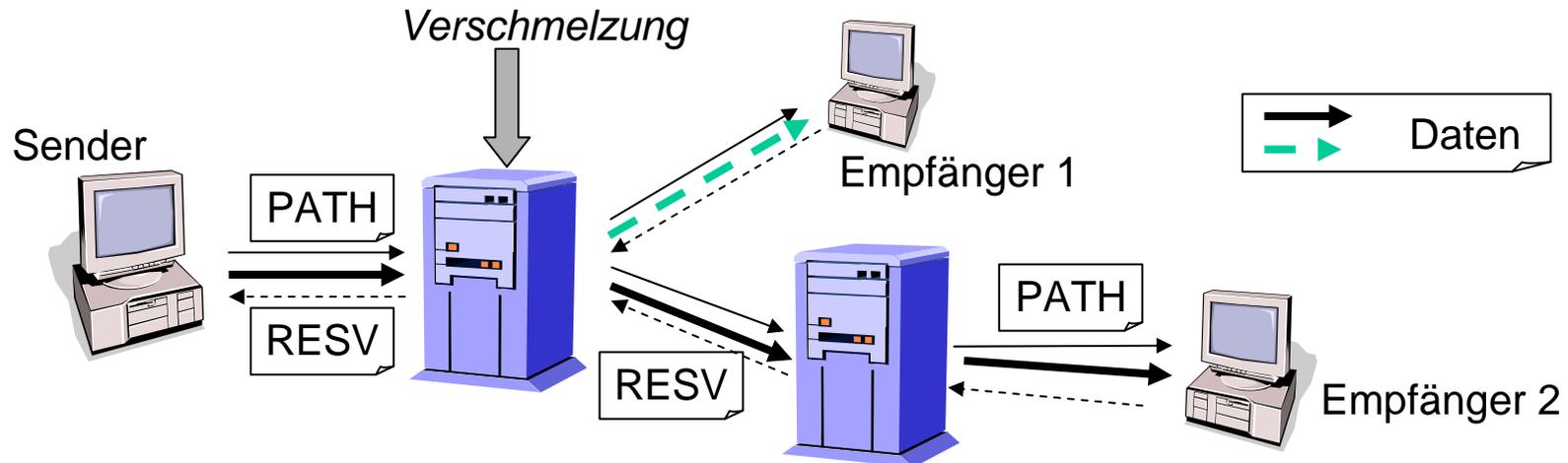
RSVP signalisiert Reservierungsanforderungen in IP-basierten Netzen.

- Der Datentransfer selbst findet weiterhin über IP statt
- Empfängerbasierte Signalisierung von Reservierungsanforderungen für unidirektionalen Datenfluss
- Unterstützung heterogener Dienstqualität, d.h. unterschiedliche Empfänger können verschiedene Dienstqualität erfahren
- Unterstützt Multicast-Kommunikation
- Unterstützung verschiedener Reservierungsstile
- Verwendet Soft-States
  - periodische Erneuerung der Zustandsdaten durch Endsysteme
  - Empfänger erhält keine positive Quittung für die Reservierung
  - Kein expliziter Abbau der Reservierungen erforderlich:  
Jeder Reservierung ist ein Zeitgeber zugeordnet nach dessen Ablauf die Reservierung gelöscht wird.

# Grundkonzepte von RSVP

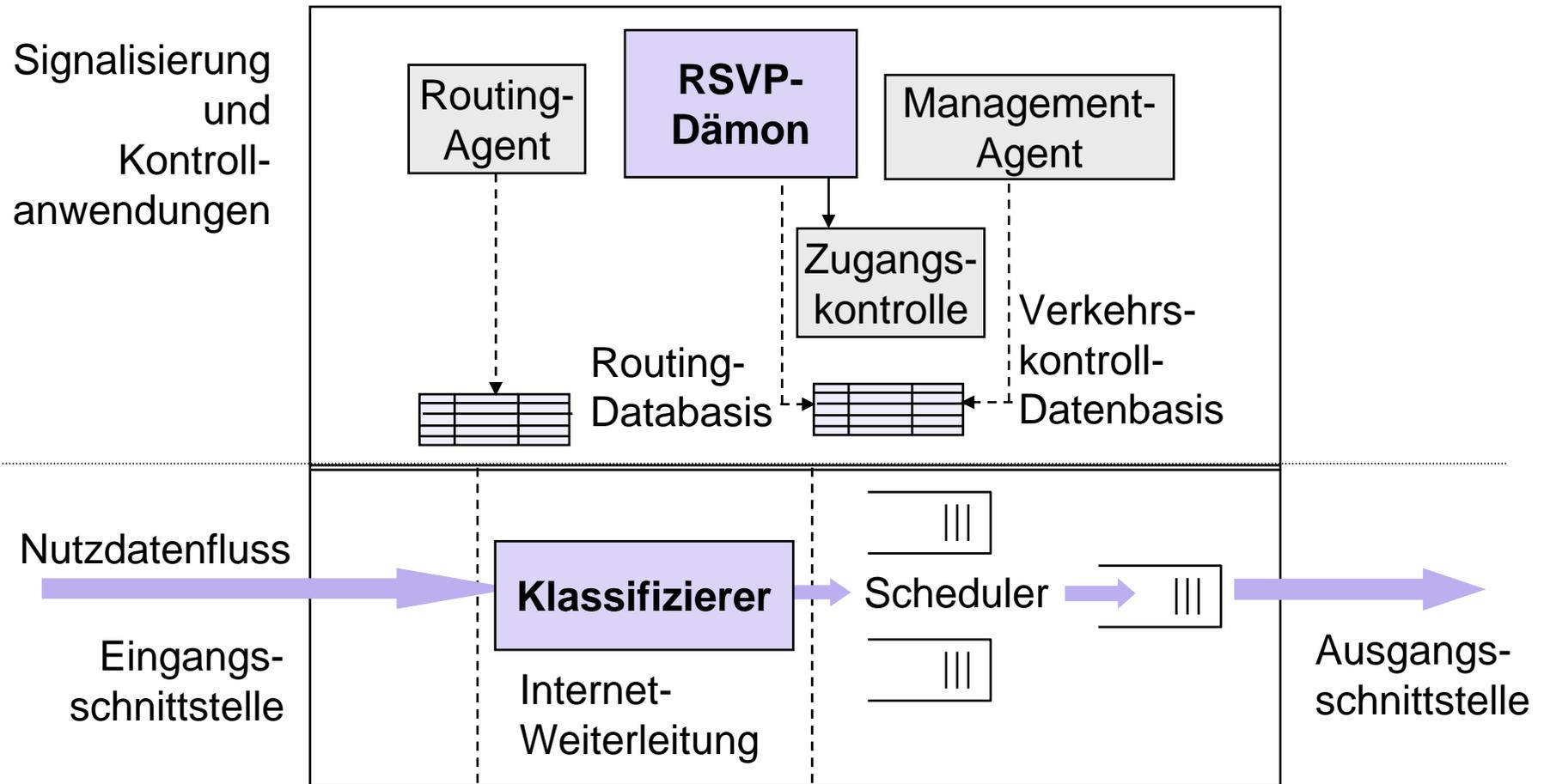
- Grundelement von RSVP ist die **Session**, d.h. eine Menge von Datenströmen mit dem gleichen Ziel (Multipeer)
  - Eine Session ist definiert durch: Ziel-IP-Adresse, Ziel-Protokoll-Kennung, Ziel-Port
- Reservierungsanforderung wird vom Empfänger der eigentlichen Daten gesendet und als **Flow Descriptor** bezeichnet. Sie besteht aus:
  - **FlowSpec** beschreibt die gewünschte Dienstqualität. (Der Inhalt der FlowSpec ist nicht Gegenstand von RSVP.)
  - **FilterSpec** beschreibt, welche Dateneinheiten einer Session die Reservierungen nutzen dürfen
- Durch die Unterscheidung von FlowSpec und FilterSpec findet eine explizite Trennung von Reservierung und Nutzung der Ressourcen statt

# Nachrichtenaustausch bei RSVP



- Sender schicken periodisch PATH-Dateneinheiten und bauen damit einen Verteilbaum auf. PATH-Dateneinheiten enthalten Information über den gesendeten Datenstrom (z.B. Dienstqualität).
- Empfänger schicken periodisch RESV-Dateneinheiten zur Reservierung der Ressourcen in Rückwärtsrichtung entlang des durch PATH-Nachrichten aufgebauten Verteilbaumes.
- Reservierungswünsche verschiedener Empfänger werden in RSVP-Routern zu einem neuen Reservierungswunsch verschmolzen, der in Richtung zum Sender weitergeleitet wird.

# Aufbau RSVP-fähiger Systeme (1)



# Aufbau RSVP-fähiger Systeme (2)

---

## Komponenten in RSVP-fähigen Systemen

- RSVP-Dämon behandelt die Signalisierung
  - Wichtig: Der RSVP-Dämon ist nicht in den Nutzdatenfluss involviert, er allein erbringt keinerlei Dienstgüte!
- Zugangskontrolle prüft, ob der Knoten die Anforderungen erfüllen kann
- Klassifizierer wählt Dateneinheiten aus, die Reservierung nutzen dürfen
- Scheduler teilt die Ressourcen zu

## Hinzu kommen die Standardkomponenten eines Routers

- Paketweiterleitung
- Routing-Engine

In der FilterSpec werden verschiedene Reservierungsstile unterschieden hinsichtlich der folgenden Aspekte:

- Speziell für jeden Sender oder gemeinsam für alle Sender

Reservierungen Kontrolle	Speziell	Gemeinsam
Explizit	<i>Fixed-Filter</i>	<i>Shared-Explicit</i>
Wildcard	...	<i>Wildcard-Filter</i>

- explizite Kontrolle der Sendermenge oder alle Sender erlaubt

Die Reservierungsstile in RSVP

- Fixed Filter: dedizierte Reservierungen für einen speziellen Sender
- Shared-Explicit Filter: gemeinsame Ressourcennutzung durch eine ausgewählte Sendermenge (Beispiel: Audioübertragung)
- Wildcard Filter: gemeinsame Ressourcennutzung durch alle Sender

Unterschiedliche Filter können nicht verschmolzen werden

## Mangelnde Skalierbarkeit

- Die Router müssen Zustandsinformationen (Qualitätsparameter, Timer, Sender- und Empfängeradressen) pro Datenstrom verwalten.
- Paketweiterleitung wird durch die erforderliche Klassifizierung eines jeden Paketes komplexer. Insbesondere im Kern des Netzes entsteht dadurch ein ggf. zu hoher Aufwand.
- Paket-Scheduling ist komplex und daher nicht so leistungsstark

## Qualitätsparameter frei wählbar

- Router muss eine sich dynamisch ändernde Anzahl von Dienstgütern unterstützen

Verletzung des KISS-Prinzips: ***Keep It Simple and Stupid***

# Differentiated Services

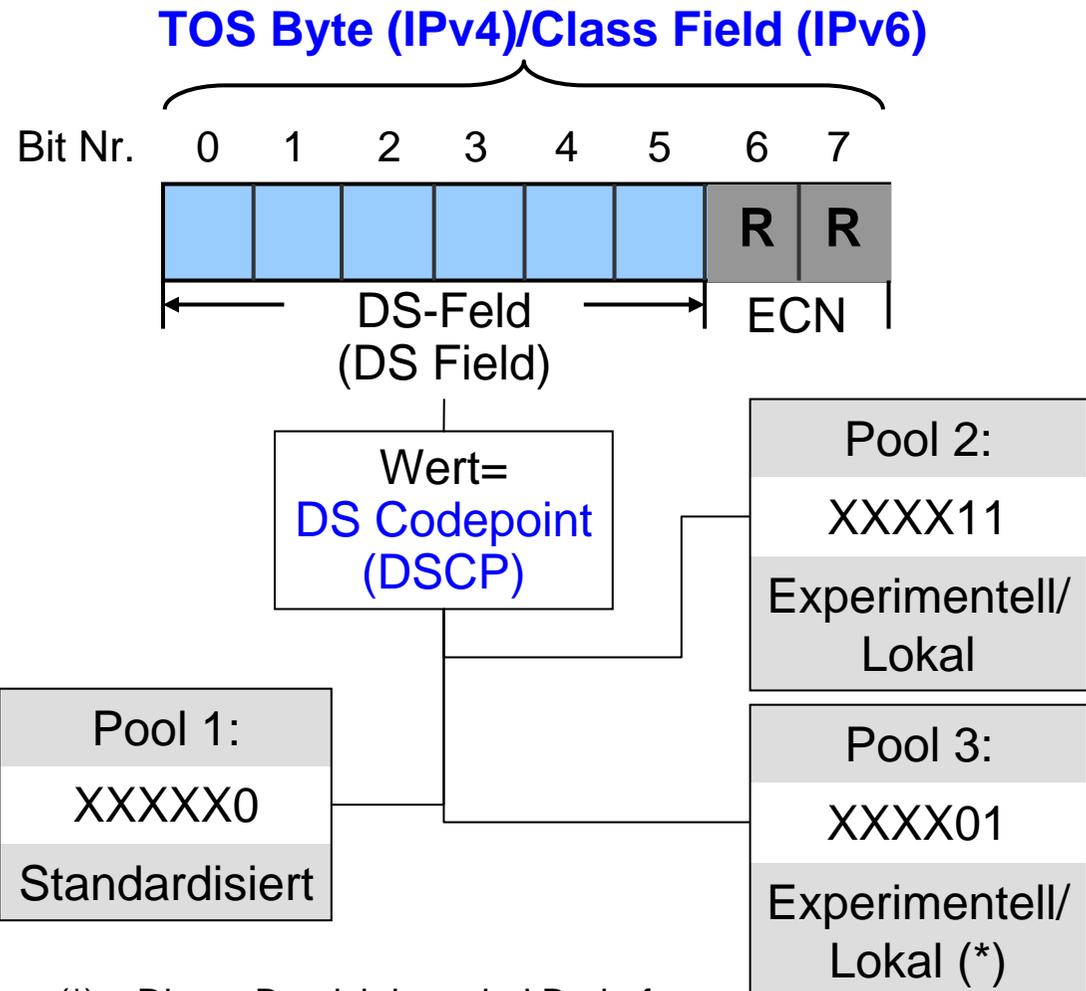
---

- 1997 erste Vorschläge, um skalierbar Dienstgüte im Internet bereitzustellen
  - Vorläuferdokument „A Two-Bit Architecture“ (siehe RFC 2638)
- Anfang 1998: IETF Arbeitsgruppe „Differentiated Services“ (bis 3/2003)
  - Qualitativ bessere, anwendungs-unabhängige Dienste mittels einfacher, skalierbarer Mechanismen
  - Reduktion der Komplexität im Netzinnern: weniger Zustände, weniger Funktionalität
  - Kompatibilität zu existierenden Anwendungen und Endsystemen (schnelle Etablierung)
  - Allerdings: nur Basismechanismen definieren, keine Dienste

- Reduktion der Komplexität durch
  - Aggregation des Verkehrs im Netzinnern zu Dienstklassen (Pakete gleicher Dienstklasse tragen entsprechende Markierung)
  - Vermeidung von Zuständen per Ende-zu-Ende-Datenstrom („Micro-Flow“) oder per Benutzer im Netzinnern (aggregierte Klassifikationszustände, einfache Paketklassifizierer)
  - „Komplexere Funktionen“ wie Klassifizierung, Markierung, Überprüfung finden nur noch an Netzgrenzen statt
- Kennzeichnung des abschnittsweisen Weiterleitungsverhaltens durch das **Per-Hop-Behavior** (PHB) im IP-Paketkopf durch **DS Codepoint** (DSCP)
- Trennung der eigentlichen Weiterleitungsmechanismen von zugehörigen Verwaltungsmechanismen (Konfiguration, Ressourcenmanagement, ...)
- Verfeinerung des ungenauen ToS-Ansatzes:
  - Explizite Rolle von Grenzknoten und verkehrsbeeinflussenden Mechanismen
  - PHB-Modell ist flexibler als relative Prioritäten oder Dienstmarkierungen

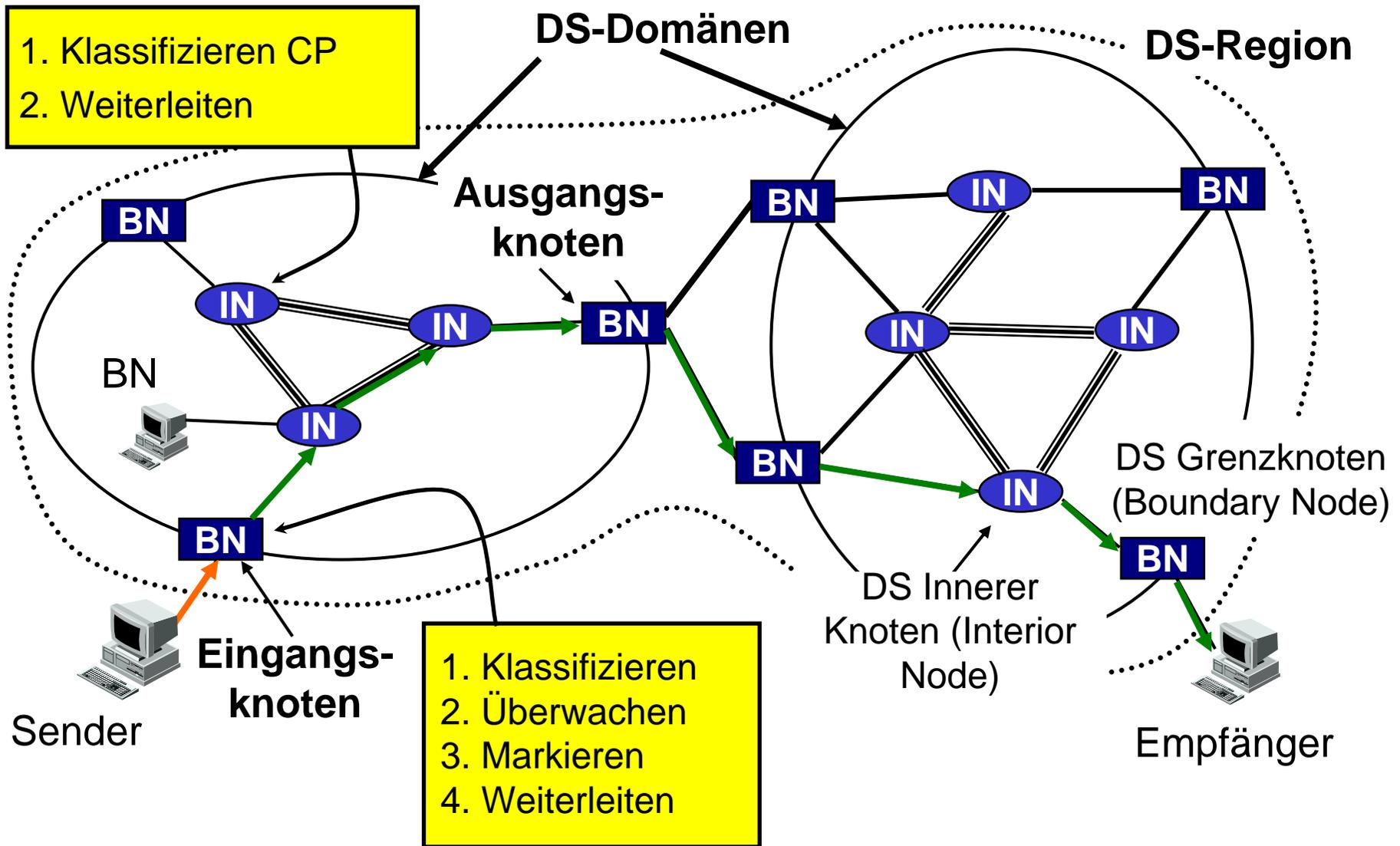
# DiffServ Codepoints

- Im IPv4- bzw. IPv6-Kopf:
- DS-Feld ist prinzipiell unstrukturiert!
- Wert des Codepoints ordnet entsprechendes PHB eindeutig zu (muss konfigurierbar sein)
- Mehrere DSCPs können auf das gleiche PHB verweisen
- Es kann mehr PHBs als DSCPs geben
- DSCP hat normalerweise keinen Einfluss auf die Wegewahl



(\*): Dieser Bereich kann bei Bedarf zur Standardisierung weiterer Werte herangezogen werden

# Differentiated Services – Überblick



## Ressourcennutzung:

- Jedes DiffServ-Paket belegt die Ressourcen eines Knotens durch das zugeordnete jeweilige PHB
- Überwachung einzelner Ende-zu-Ende-Datenströme erfolgt üblicherweise nur im ersten Grenzknoten
  - Verkehrsprofil im ersten Grenzknoten entscheidet über Markierung des Pakets und damit über die weitere Ressourcennutzung
  - Innere Knoten besitzen (normalerweise) keine Verkehrsprofile, d.h. Ressourcennutzung kann dort nicht überwacht werden
  - Anschließend kann also nur noch das Gesamtverhalten von Aggregaten in Grenzknoten überwacht werden, nicht jedoch das Verhalten einzelner Micro-Flows
  - Eventuell IPSec Authentifizierung zur Sicherung der Herkunft einsetzen

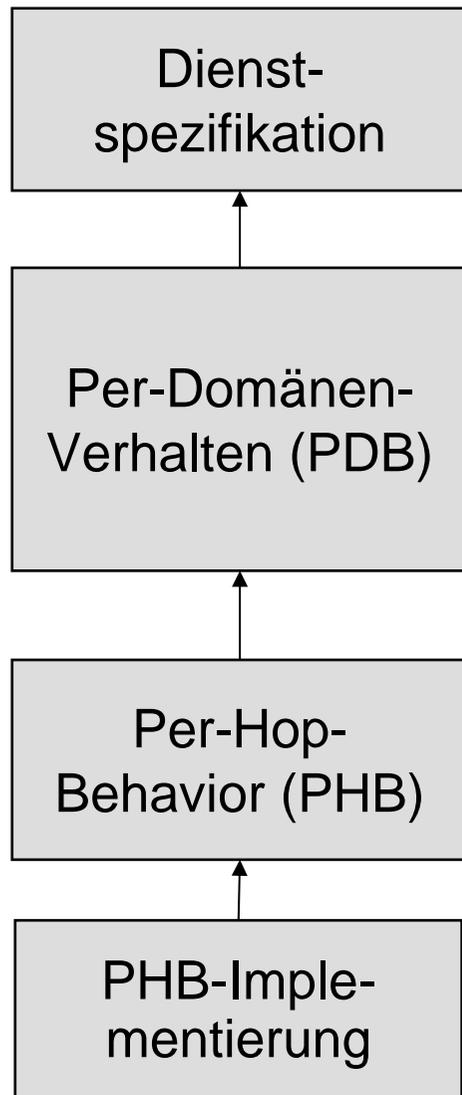
## Ressourcenreservierungen:

- Üblicherweise per Aggregat
- Anfangs (d.h. beim „Rollout“): statische Reservierung durch manuelle Konfiguration des Netzbetreibers (ermöglicht frühzeitigen Einsatz)
- Später: möglichst dynamisch, on-demand (benötigt Signalisierung)
- Initiale, eher statische Aufteilung der Ressourcen zwischen den verschiedenen PHBs („Ressourcenpartitionierung“) für Knoten
- Über belegte bzw. freie Ressourcen müssen nicht die Knoten selbst Buch führen
- Freigabe zur Nutzung der reservierten Ressourcen erfolgt durch Installation eines entsprechenden Profils im ersten Knoten (ist somit wichtig für die Sicherheit)

# Differentiated Services – Dienste (1)

- Konstruktion eines Dienstes durch:
  - Per-Domain-Behavior (PDB) setzt sich zusammen aus
    - Weiterleitungsmechanismen (PHB, d.h. Warteschlangen und Scheduler) und
    - Regeln zur Verkehrsbeeinflussung (Klassifizierer, Messelemente, Former,...)
  - Ende-zu-Ende-Dienst durch Verkettung von mehrere PDBs
  - Somit Bausteinhierarchie: PHB → Per Domain Behavior → Dienst
- Dienstleistungsvereinbarung (Service Level Agreement – SLA):
  - Dienstvertrag zwischen Dienstkunde und Dienstbetreiber, der den Weiterleitungsdienst festlegt, welchen der Kunde erhalten sollte
- Komponenten zur Realisierung eines Dienstes:
  - PHB-Implementierungen (konkrete Realisierung eines PHBs)
  - Verkehrsbeeinflussungsmaßnahmen (Traffic Conditioning)
  - Bereitstellungsstrategien und Abrechnungsmodelle

## Differentiated Services – Dienste (2)



Ende-zu-Ende-Dienste:

- Spezifikation über Service Level Specification
- Kombination aus den PDBs der besuchten Domänen

Domänenweites Weiterleitungsverhalten:

- PHB-Spezifikation und verkehrsbeeinflussende Mechanismen (Traffic Conditioning)
- Attribute beschreiben Eigenschaften
- Beschreibung von Aggregationseffekten

Abschnittsweises Paketweiterleitungsverhalten:

- Paketbearbeitung innerhalb eines Knotens
- 

Implementierung des Weiterleitungsverhalten:

- Warteschlangen- und Schedulingmechanismen

## Differentiated Services – Dienste (3)

---

- Bilaterale Dienstverträge zwischen benachbarten Internet Service Providern
  - statisch oder dynamisch
- Technische Dienstspezifikation:
  - Leistungsparameter, z.B. Durchsatz, Verzögerung, Verlust
  - Topologischer Gültigkeitsbereich
  - Verkehrsprofil, z.B. Rate und Burstlänge
  - Markierungs- und Verkehrsformungsverhalten
  - Zusätzlich allgemeine Parameter, z.B. Verfügbarkeit, Zuverlässigkeit, Wegebeschränkungen
- Service Level Agreements (SLA) enthalten darüber hinaus noch geschäftliche bzw. wirtschaftliche Aspekte, z.B. Bedingungen für Regresszahlungen, etc.

- **Per-Hop Behavior (PHB):**
  - extern sichtbares Verhalten von Paketen in einem DS-Knoten
  - bestimmt Behandlung von Paketen anhand DSCP während der Weiterleitung innerhalb eines DS-Knotens
- Bisher standardisierte PHBs:
  - „Default PHB“ ist das bisherige Best-Effort-Verhalten
  - Class Selector PHBs, siehe RFC 2474:
    - kompatibel zu IP-Precedence-Feld im ToS-Byte
    - Acht relative Prioritätsklassen (inkl. Default-PHB)
    - Je größer der Wert, desto höher die Priorität
  - Expedited Forwarding PHB, siehe RFC 3246
  - Assured Forwarding PHB

# Expedited Forwarding PHB

- Ausgangspunkt:
  - Idee der virtuellen Standleitung, d.h. garantierte Bandbreite und kein Jitter
- Expedited Forwarding PHB als Basis für Dienste mit geringer Verzögerung geringen Paketverlusten
  - garantierte Bandbreite
  - niedriger und begrenzter Jitter
- Ziel
  - ankommende Pakete „sehen nur leere Warteschlangen“
  - Paket verlässt den Router „sofort“ wieder
- Summe der Ankunftsrate muss kleiner als die minimale Ausgangsrate sein → Zugangskontrolle notwendig
- Implementierung z.B. durch Simple Priority Queueing oder WFQ

Bemerkung: Ursprüngliche Spezifikation in RFC 2598 ungenau,  
daher Neudefinition in RFC 3246 (weitere Erläuterungen dazu in RFC 3247)

# Assured Forwarding PHB (1)

- **Assured Forwarding PHB Group** [RFC 2597]
  - Definiert Eigenschaften für „AF-Typ“
- **AF-Klasse:**
  - Instanz eines AF-Typs
  - Gruppe aus m PHBs mit je unterschiedlicher Verwurfspriorität
  - Vorgeschlagen: m=3, d.h. Verwurfsprioritäten niedrig, mittel, hoch; mindestens 2 unterschiedliche Prioritäten je AF-Klasse gefordert
  - keine Umordnung von Paketen eines Micro-Flows zugelassen
  - vollständig unabhängig von anderen AF-Klassen
- n unabhängige AF-Klassen (4 mit standardisierten DSCPs)

Verwurfspriorität (y)	AF 1y	AF 2y	AF 3y	AF 4y
<b>Niedrig (1)</b> ●	001010	010010	011010	100010
<b>Mittel (2)</b> ●	001100	010100	011100	100100
<b>Hoch (3)</b> ●	001110	010110	011110	100110

AF-Klasse

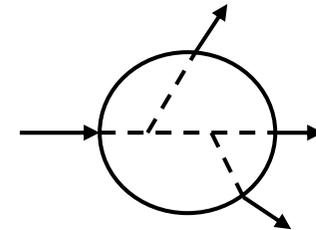
## Assured Forwarding PHB (2)

---

- Aktives Warteschlangenmanagement (z.B. RED) gefordert
- Verwurfswahrscheinlichkeiten für PHBs müssen zwischen Betreibern aus Konsistenzgründen abgestimmt werden
- Basis für Dienste mit
  - zugesicherter Bandbreite unterhalb vereinbarter Senderate (Garantie)
  - Nutzung weiterer Bandbreite, falls diese verfügbar
  - bevorzugtem Verwerfen von Paketen oberhalb der vereinbarten Senderate bei Ressourcenmangel
  - stoßartigem Verkehr, längere Bursts haben höhere Verwurfswahrscheinlichkeit
- Oberhalb zugesicherter Rate: statistisches Multiplexing zwischen Flows

# DiffServ-Bausteine: PDBs

- **Per Domain Behavior (PDB)** [RFC 3086]:
  - Ein Per-Domain-Behavior beschreibt das Verhalten, das Pakete auf ihrem Weg durch eine DS-Domäne erfahren:
    - beliebiger Eingang zu beliebigem Ausgang (One-to-One)
    - beliebiger Eingang zu jedem Ausgang (One-to-Any)
    - beliebiger Eingang zu bestimmten Ausgängen (One-to-Few)
  - Regeln zur Verkehrsbeeinflussung (Traffic Conditioning) und zu verwendende PHBs müssen angegeben werden
  - Berücksichtigung der Aggregationseffekte
  - Attribute, die PDB charakterisieren, messbar und quantifizierbar
  - „Vorstufe“ eines Dienstes



- Nachbildung dedizierter physikalischer Leitung bestimmter Bandbreite
- Attribute:
  - garantierter Durchsatz
  - obere Schranke für Delay-Jitter
- Verkehrsbeeinflussung:
  - Strikte Überwachung (Policing) am Eingang (nicht-konforme Pakete verwerfen)
  - Shaping am Ausgang einer Domäne
- Ziel: Einhalten eines so genannten Jitter-Window, so dass obere Jitter-Schranke garantiert wird
- Vorgehen: Verzögern des ersten Pakets um maximales Jitter-Window  
→ Zeit zum Ausgleichen von Schwankungen wird gewonnen,  
aber: zusätzliche u.U. unnötige Verzögerung der Pakete
- basierte noch stark auf alter EF-PHB-Definition, daher überholt

## PDBs: Assured Rate (1)

---

- Zugesicherte Rate wenn Sender bis zu dieser Rate (Committed Information Rate – CIR) sendet
- Attribute:
  - zugesicherte Rate
  - niedrige Verwurfswahrscheinlichkeit für ratenkonformen Verkehr
- keine Zusicherung von Delay- oder Jitter-Schranken
- Ausnutzung weiterer verfügbarer Bandbreite möglich (aber nicht garantiert)
- Zugesicherte Rate wird unabhängig vom Verkehrstyp (z.B. UDP/TCP) erbracht, Trennung von UDP/TCP möglich
- Nutzung einer AF-Klasse

## PDBs: Assured Rate (2)

---

- Ermittlung und Anpassung an zusätzlich nutzbaren Bandbreitenanteil gut mit TCP möglich
- Verkehrsbeeinflussung:
  - Klassifizierung, Messen (genaue Methode muss spezifiziert werden) und Markieren am Eingang
  - Traffic Shaping am Eingang nicht notwendig
- Messmethoden für zugesicherte Rate „CIR“:
  - Committed Burst Size (CBS) über Zeitintervall T1
  - Peak Information Rate (PIR), Peak Burst Size (PBS), Excess Burst Size (EBS), ggf. weiteres Zeitintervall T2
- Markierung als „grün“, „gelb“ und „rot“:
  - Verwerfen roter Pakete am Eingang durch Überwacher (Policer) möglich
  - Verwerfen gelber Pakete erfolgt hingegen nicht durch Eingangsüberwachung (Ingress-Policer), sondern nur durch PHB-Mechanismus
  - Verwerfen grüner Pakete erst nachdem alle gelben und roten Pakete verworfen wurden

- Anwendung Assured-Rate-basierter Dienste
  - Datenübertragung mit zeitlicher Obergrenze
  - Video-Playback: variable Bitrate, Jitter-Kompensation möglich
  - Kopplung virtueller privater Netze mit Mindestgarantie
- Anwendung Virtual-Wire-basierter Dienste
  - Kopplung virtueller privater Netze mit Qualität einer dedizierten Standleitung
  - Voice over IP
  - Interaktive (Audio/Video-) Anwendungen
- Notwendige Schritte beim Betreiber:
  - Auswahl der PHBs, ihrer Implementierung und deren Parameter, Verhältnis zu anderen PHBs (Ressourcen-Partitionierung)
  - Auswahl konkreter „Traffic Conditioning“-Mechanismen
  - SLA und „Traffic Conditioning Agreement“ mit anderen Betreibern und Kunden abstimmen
  - Routerkonfiguration (PHBs und Profile)
  - Messung und Überwachung der erreichten Qualität

# We don't need no reservation

---

## *The Call*

*(to the tune of Pink Floyd's „The Wall')*

We don't need no reservation  
We don't need ad-mission control  
All applications must be adaptive  
The Net works just fine, so, leave it alone  
Hey, Professor, leave the Net alone!  
All we want is just, flat rate pricing for all

We don't need no traffic management  
Overprovision bandwidth for all  
The only true god is TCP/IP  
The Net isn't broken, so leave it alone  
Hey Professor, leave that Net alone!  
All we want is just to make the router code small

S. Keshav

# Differentiated- & Integrated-Services

	Best-Effort	Integrated-Services	Differentiated Services
QoS-Garantie	keine	pro Datenstrom (Microflow)	für aggregierte Datenströme
Konfiguration	keine	pro Datenstrom bzw. Sitzung	pro Aggregat zwischen Domänen
Typ der Garantie	keine	individuell per Datenstrom	aggregiert
Dauer der Garantie	keine	kurzlebig (Sitzungsdauer)	langfristig(er)
Zustands-haltung	keine	pro Datenstrom	pro aggregierter Reservierung
Signalisierung	keine	RSVP	Keine, bzw. noch nicht definiert
Multicast-Unterstützung	IP-Multicast	Empfängerorientiert, heterogen	IP-Multicast, aber Reservierungsprobleme

Im Sommersemester („*Internet-Protokolle 2*“):

- Ad-Hoc-Kommunikation & Sensornetze
- Peer-to-Peer Computing

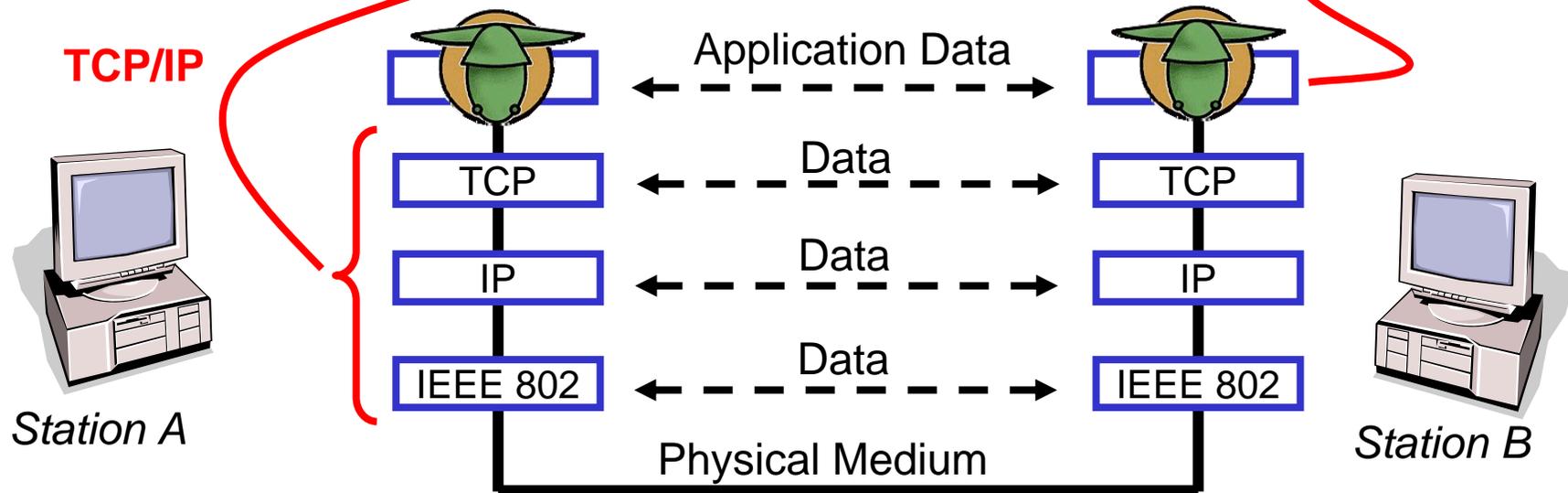
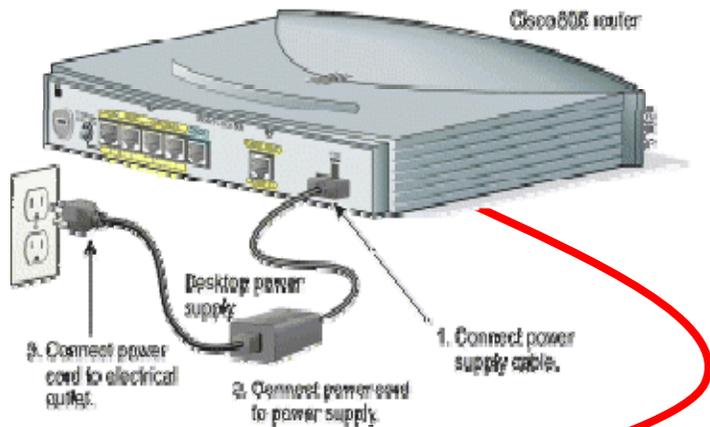
Außerdem:

- Praktikum!?!

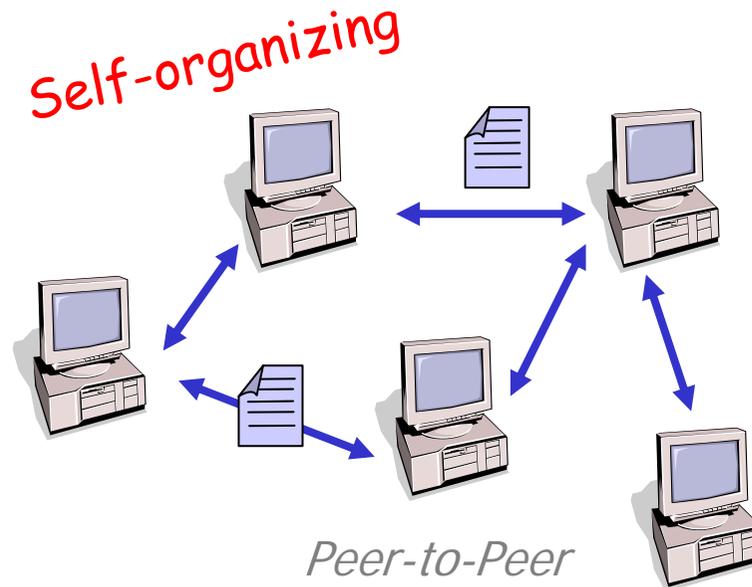
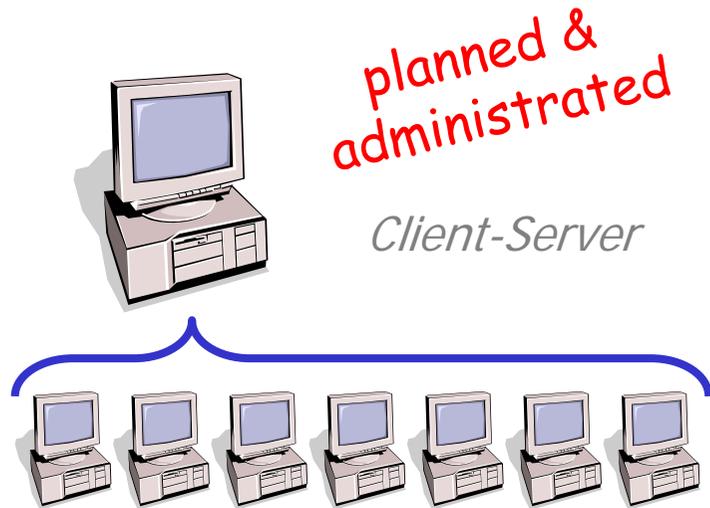
Jederzeit:

- Bachelor-, Master- und Diplomarbeiten
- SEPs, Guided Research
- Praktikum!?!
- Hiwi-Jobs, z.B. Protokollimplementierungen, etc.

# What's Peer-to-Peer? (1)



# What's Peer-to-Peer? (2)



Peer-to-Peer ...

## Organic Growth

- Each machine contributes.
- Joining devices provide the resources they consume

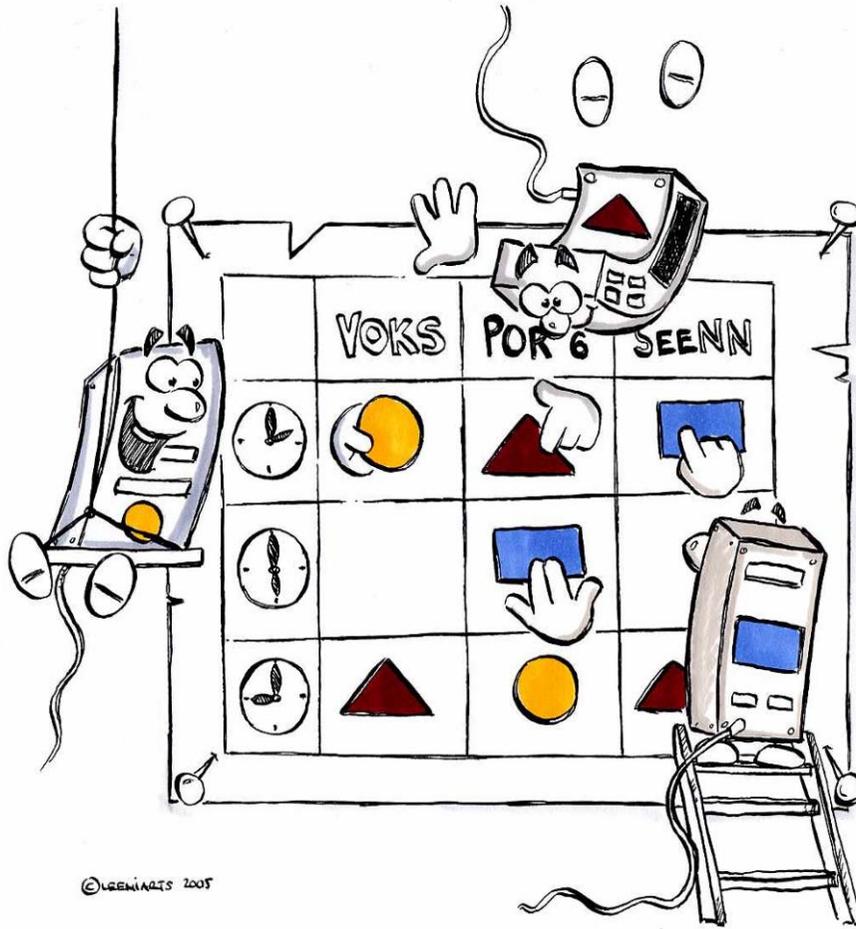
## Robust and Fault-Tolerant

- No single point of failure

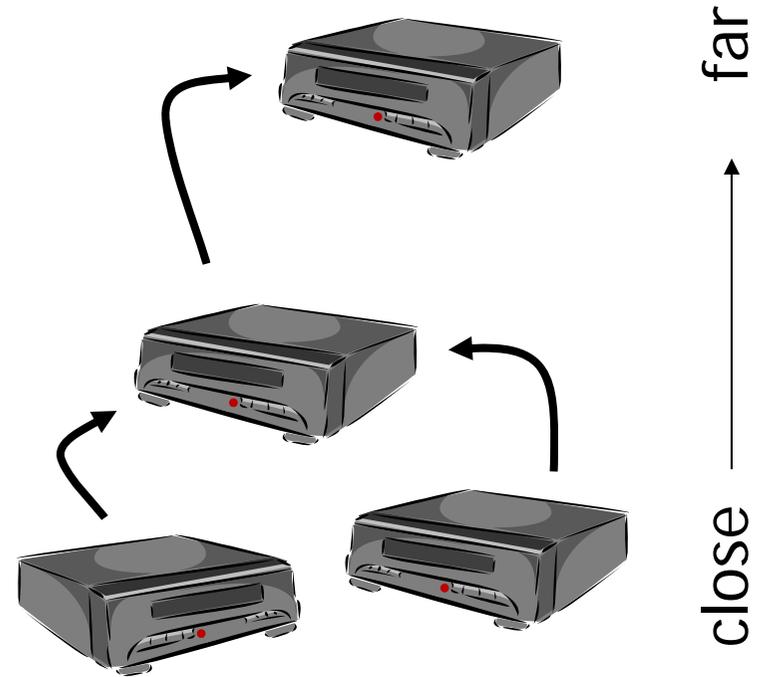
## Research Question:

- Which rules make the peer-to-peer system behave as desired?

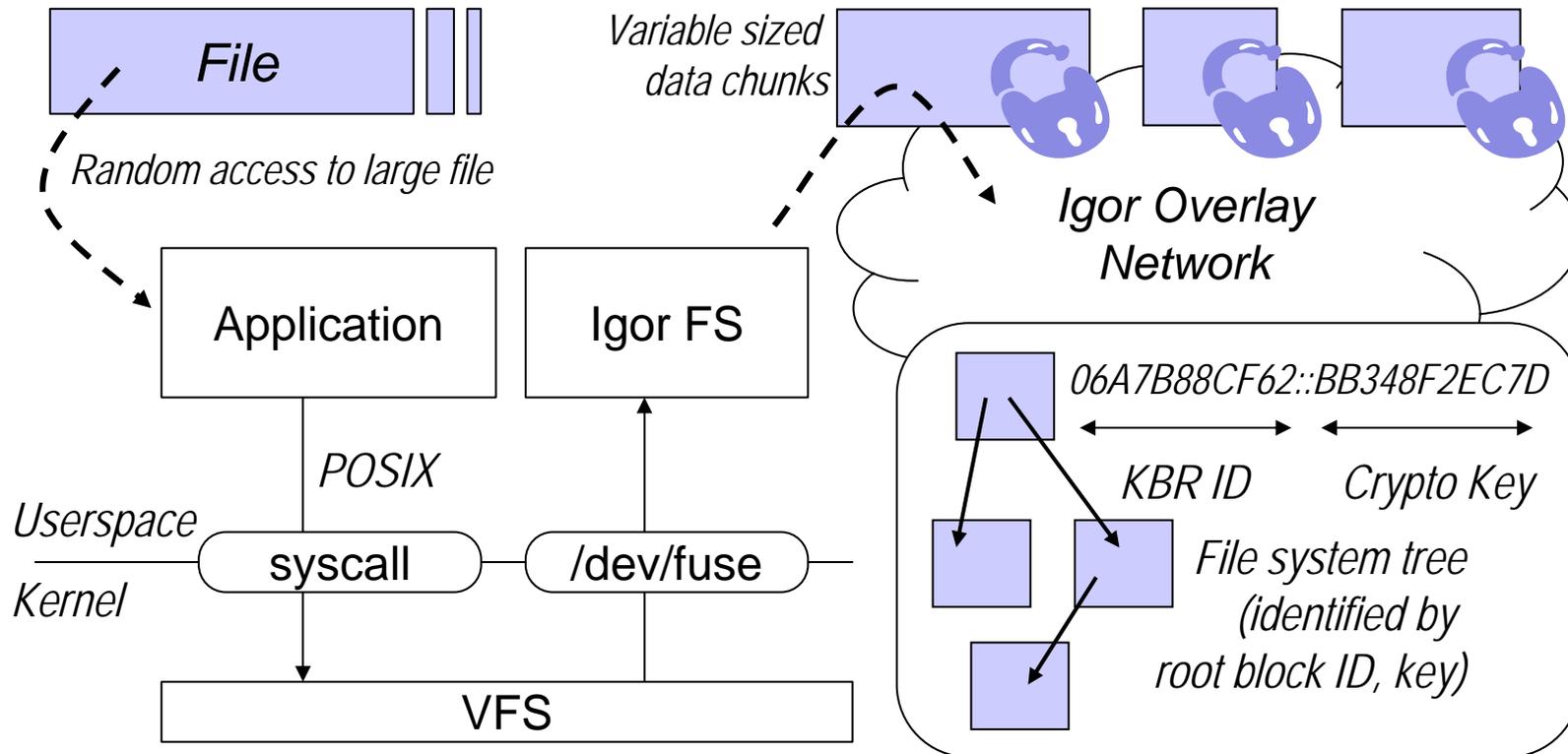
# Peer-to-Peer Video Recorder „Videgor“



*Videgor:*  
Decentralized Storage & Scheduling

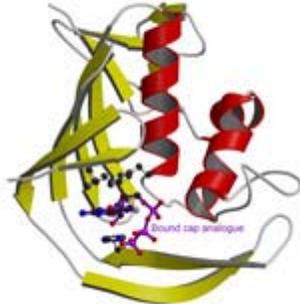


# The IGOR File System



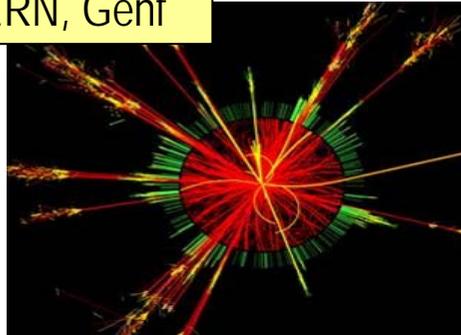
# Anwendungsgebiete von Igor FS

EMBL, Heidelberg



- Große Dateien in der Bioinformatik
- Mehrere zentrale Datenquellen (für getrennte Verzeichnisse)
- Häufige, kleine Änderungen
- Viele Abonnenten, die jeweils nur kleine Abschnitte der Dateien lesen

CERN, Genf



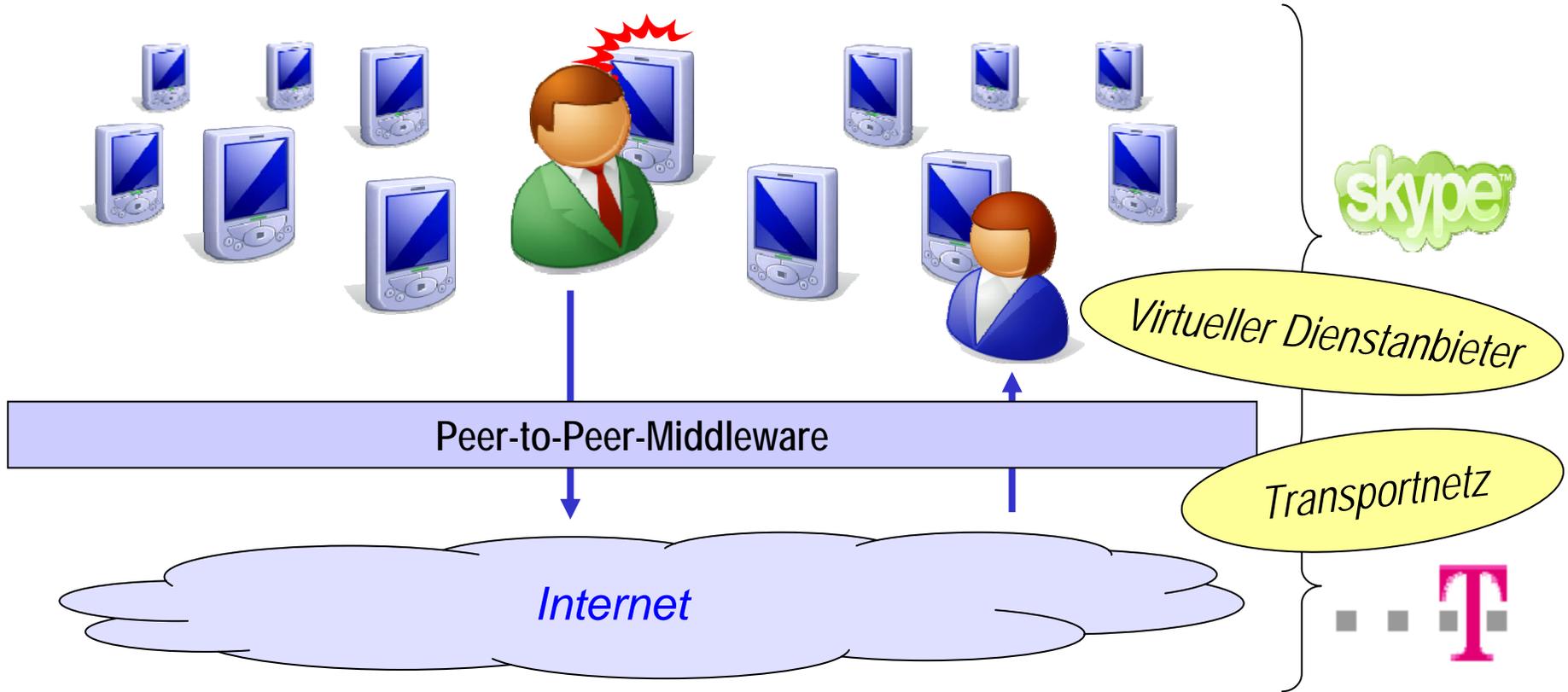
- Große Zahl von Konfigurationen (OS + Bibliotheken + Analyse-Software)
- Große Zahl von Rechnern im Cluster
- Häufige Konfigurationswechsel, Cold Standby, etc.
- Robust & Effizient → Dezentralität



- Verteiltes Dateisystem für allgemeine Anwendungen
- Benutzer, Gruppen
- Konflikte?
- Fairness?

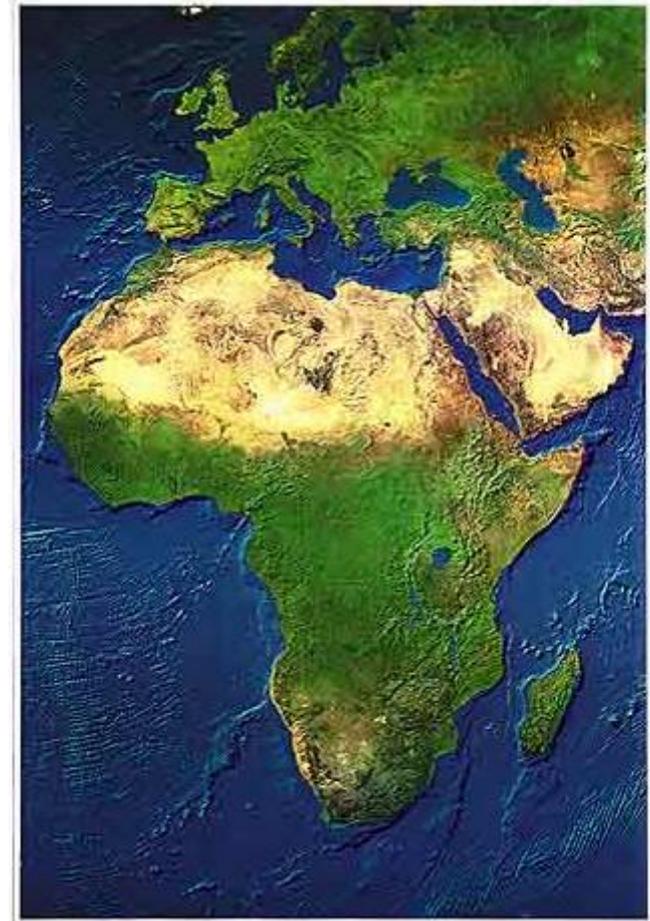
Aktuelle Arbeiten

# P2P ermöglicht virtuelle Dienstleister

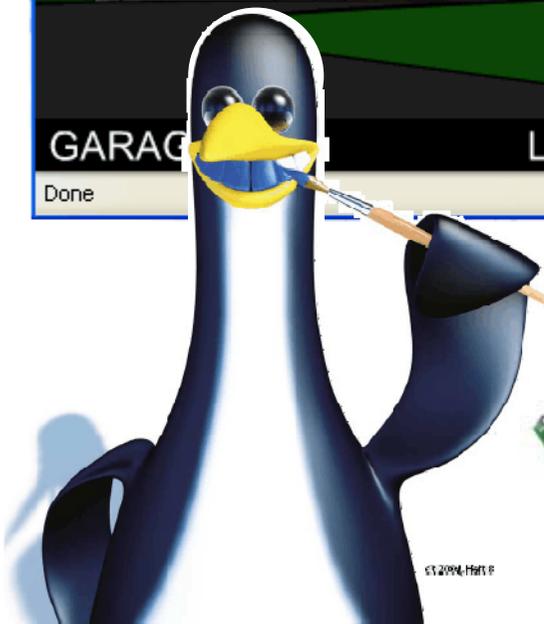




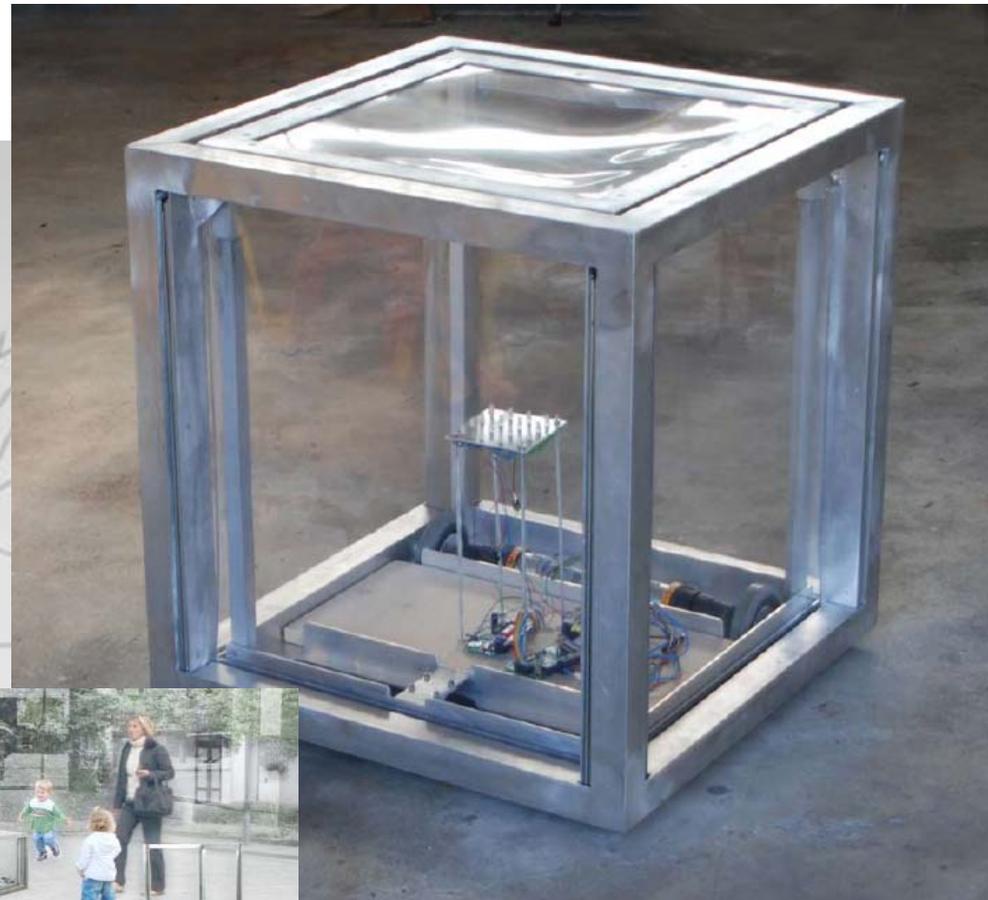
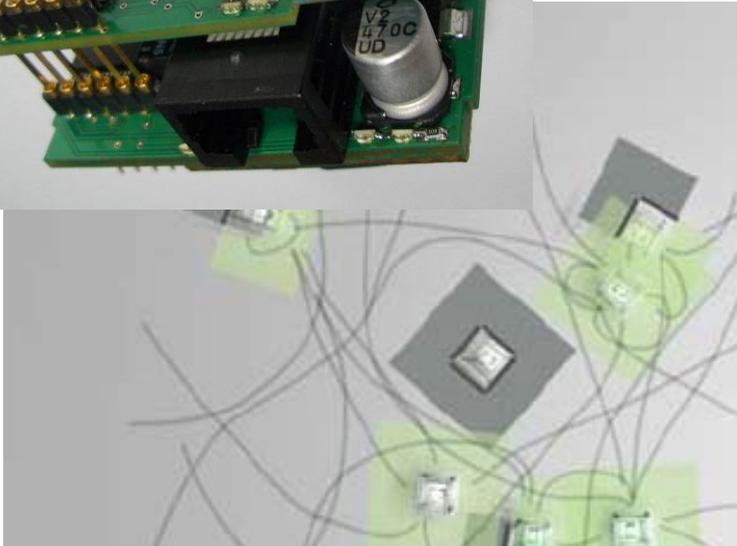
*Große Ad-hoc- und Mesh-  
Netze ermöglichen die  
Versorgung dort wo keine  
Infrastruktur zur  
Verfügung steht.*



# Ambient Computing



# Fernfühler – Autonom agierende Objekte



# High Performance Computing ...

*Seymour Cray:*

*If you were plowing a field, which would you rather use: Two strong oxen or 1024 chickens?*



HLRB Garching (rechts oben), Mare Nostrum (oben), NASA Columbia (rechts)

---

# Questions?



Thomas Fuhrmann

Department of Informatics  
Self-Organizing Systems Group  
c/o I8 Network Architectures and Services  
Technical University Munich, Germany

[fuhrmann@net.in.tum.de](mailto:fuhrmann@net.in.tum.de)