WS 2011
LV Informatik-I für Verkehrsingenieure

# 7. Rechnernetze
## 7.1 Architektur

Dr. rer.nat. D. Gütter

Mail: Dietbert.Guetter@tu-dresden.de
WWW: wwwpub.zih.tu-dresden.de/~guetter/

# Definition

Ein **Rechnernetz**

ist ein System von Computern,
zwischen denen ein automatischer Nachrichtenaustausch möglich ist.

Die Kommunikation erfolgt dabei nach standardisierten Vorschriften.

Der Nutzen eines Rechnernetzes ergibt sich aus

- **Kommunikationsverbund**
  dient dem Nachrichtenaustausch aller Rechner im Netz

- **Ressourcenverbund**
  gemeinsame Nutzung von Hard- und Softwarekomponenten
  z.B. von Netzwerkdruckern oder von Datenbanken.

- **Steuerungsverbund**
  verteilte Verarbeitung auf mehreren Computern
  z.B. Fabrikautomatisierung, Reduktion Verarbeitungszeit

# WAN und LAN

**WAN** (Weitverkehrsnetz, bzw. flächendeckende Rechnernetze)

- unbegrenzte Netzausdehnung und Rechneranzahl
- realisiert ab 1969 (ARPANET)

**LAN** (Lokale Rechnernetze)

- begrenzte Netzausdehnung und Rechneranzahl
- realisiert ab 1980 (Ethernet)

**MAN** (Stadtnetze), Zwischenstellung zwischen WAN/LAN

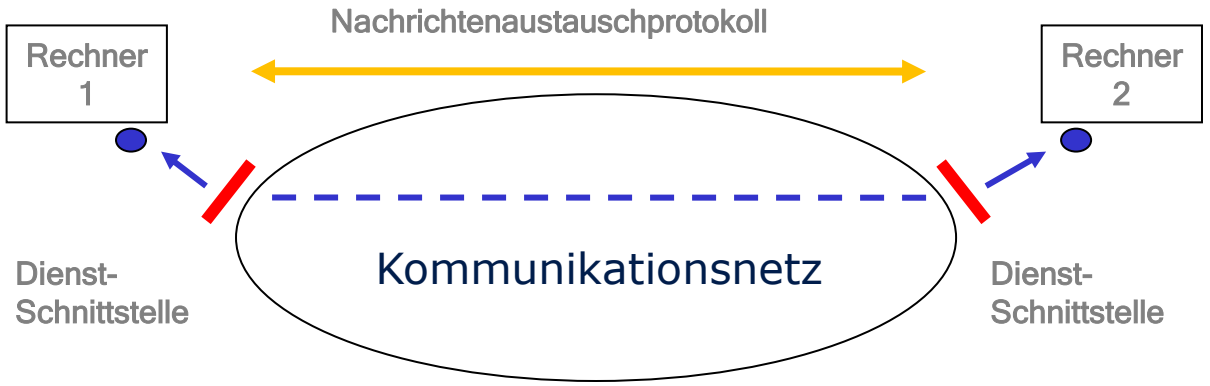
**Trends**

- Auflösung der Grenzen zwischen LAN und WAN
  durchgängige Vernetzung

# Rechnernetzdienste und -Protokolle

**Rechnernetzprotokolle**
standardisierte Nachrichtenübertragung festgelegt werden

- Nachrichtensyntax
- zulässige Nachrichtenreihenfolge
- Zeitschranken
- Fehlerreaktionen




**Rechnernetzdienste**
Dienstleistungen, charakterisiert durch

- Dienstspezifikation
- Dienstschnittstelle, Diensterbringung ist transparent
- Diensthierarchie

# proprietäre Systeme

1960-er Jahre

- Rechenzentren experimentieren mit Rechnerverbundsystemen
- Einzellösungen, i.a. nicht nachnutzbar

1970 - 1990

- Netzwerkarchitektur SNA von IBM, seit 1974
- Netzwerkarchitektur DNA/DECnet von DEC, nach 1975
- Netzbetriebssystem Novell Netware (für LAN), 80-er Jahre

i.a. Familien-Architektur eines Herstellers

- proprietäre Dienste und Protokolle

➔ keine Zusammenarbeit mit Rechnern anderer Hersteller

# offene Systeme

In den 1970-er Jahren entstand die Forderung
nach herstellerneutraler Vernetzung (**offene Systeme**)

Standards müssen verbindliche Festlegung enthalten

- Hardwarekopplung (Kabel, Steckerformen, Spannungen, …)
- Protokolle und
- Dienstleistungen

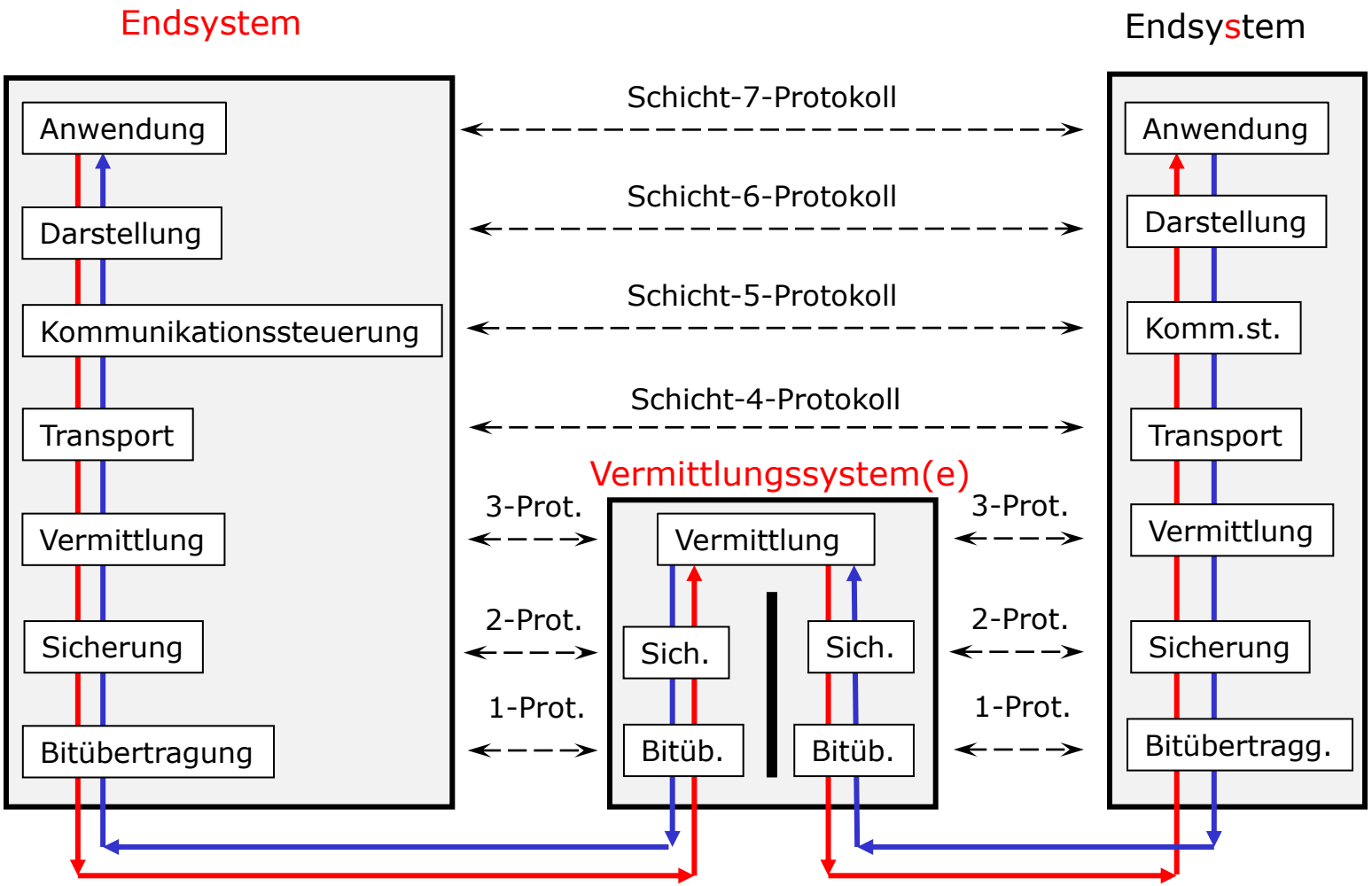
Standards dürfen keine Festlegungen enthalten über

- Rechnerarchitektur
- Betriebssystemarchitektur

➔ 2 dominante Architekturmodelle

- **OSI**-Referenzmodell der ISO (International Standards Organisation)
- Arpanet/Internet des **DoD** (U.S, Department of Defense)

# ISO/OSI-Modell (Open System Interconnection)



# ISO/OSI-Modell

- Endsysteme besitzen 7 Schichten, jeweils
  - Dienstschnittstellen mit adressierten Dienstzugriffspunkten
  - Instanzen zur Dienstausführung mit internen Ausführungsprotokollen
- Endsysteme können direkt gekoppelt sein,
  in der Regel sind sie aber über (mehrere) Vermittlungssystem gekoppelt.
- Vermittlungssystem besitzen nur 3 Schichten
  - Wegewahl (Routing) in komplexen Systemen
  - Dienstqualität (Verluste, …) unterschiedlich je nach Netzwerktyp
- Transportschicht sichert Übertragungsqualität (Ende-zu-Ende-Steuerung)

→ Übertragungsorientierte Schichten: 1-4
Verarbeitungsorientioerte Schichten: 5-7

# Bitübertragungsschicht

**Aufgabe**
Übertragung beliebiger Bitströme über Kommunikationskanal

**Ziel**
optimale Nutzung eines konkreten physikalischen Übertragungsmediums

**Standards**
enthalten mechanische, elektrische, optischen  Festlegungen, …

z.B.

- Vorschriften zu Kabelarten
- Steckerformen
- Impulsspannungen
- Taktraten
- Synchronisationsmechanismen

# Sicherungsschicht

**Aufgabe**
sichere Nachrichtenübertragung über Bitübertragungsschicht

**Frames**
Nachrichten der Sicherungsschicht Frames bzw. Rahmen

Rahmen enthalten redundante Informationen für

- Erkennung Rahmenanfang und –ende
- Erkennung von evtl. Bitverfälschungen

Gewährleistung der Übertragungssicherheit

- Quittierung des korrekten Nachrichtenempfanges
- Übertragungswiederholung im Fehlerfall
- Duplikatserkennung

# Vermittlungsschicht

**Aufgabe**
Nachrichtenübertragung in Kommunikationsnetzwerken

- trivial, wenn Quell- und Zielrechner direkt gekoppelt
- nicht trivial,
  wenn Quell- und Zielrechner über Vermittlungsrechner gekoppelt

Leitwegbestimmung (**Routing**)

- Mehrere Möglichkeiten der Nachrichtenvermittlung
- Auswahl des günstigsten Weges

**Adreßanpassungen** bei heterogenen Netzen

Sammeln von **Abrechnung**sinformationen.

# Transportschicht

**Aufgabe**
sichere und effiziente Nachrichtenübertragung auf end-to-end-Niveau
höchste datenübertragungsorientierte Schicht

Ausgleich evtl. **Mängel der Vermittlungsschicht**

- Nachrichtenverluste
- Reihenfolgeverletzungen
- Verbindungsabbrüche
- Nachrichtengrößenanpassung

Nachrichtenflußsteuerung
evtl. Dienstgütegarantie (Mindestdurchsatz, Übertragungsdauer, …)

Multiplexen mehrerer virtueller Transportverbindungen

# Kommunikationssteuerungsschicht

auch Sitzungschicht

**Aufgabe**
Koordinierung der Datenverarbeitung

Nachrichtenübertragungsverbindungen mit Nutzerunterstützung bezüglich

- Dialogverwaltung
  simplex / duplex / halbduplex
- Synchronisierung
  Sicherungspunkte für evtl. Rücksetzen während einer „Sitzung“
- Aktivitätsverwaltung
  Einteilung einer “Sitzung” in sinnvolle Abschnitte

# Darstellungsschicht

**Aufgabe**
Unterstützung der Verständigung von Anwendungsschichtinstanzen

- Datenaustausch zwischen heterogenen Rechnern im Netz

  evtl. unterschiedliche Informationsdarstellungen
  Konvertierungen der Darstellungen vornehmen

- Extrem umfangreiche Übertragungsdaten

  evtl. Komprimierung

- Vertraulichkeit von Übertragungsdaten

  evtl. Verschlüsselung

# Anwendungsschicht

**Aufgabe**
beinhaltet direkt nutzbare Anwendungen

- Dateitransfer
- E-Mail
- Computerfernbedienung

- Verteilte Verarbeitung
- Verteilter Zugriff auf Dokumente, Datenbanken, …
- Suchmaschinen
- spezielle Dienstleistungen

- Multimediaübertragung

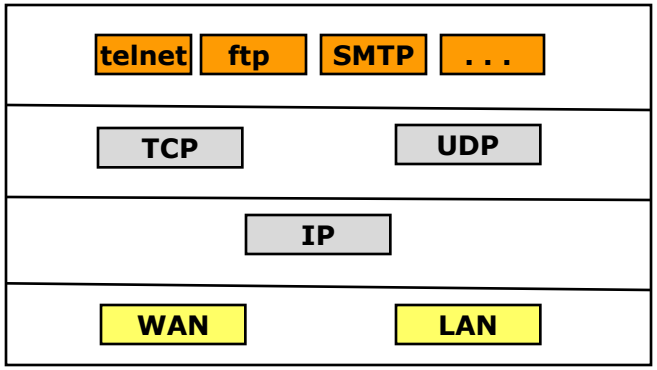
- Programmierunterstützung für Anwendungsprogrammierer
  fertige Bausteine

# Arpanet / Internet

1969

- einfache, offene Rechnernetzarchitektur
  gefördert durch US-Verteidigungsministerium (DoD)
- zunächst Kopplung von 4 Rechenzentren
- schrittweise Weiterentwicklung → Internet

1980er Jahre
Internet Netzwerkarchitektur




**Anwendungsschicht**

**Transportschicht**

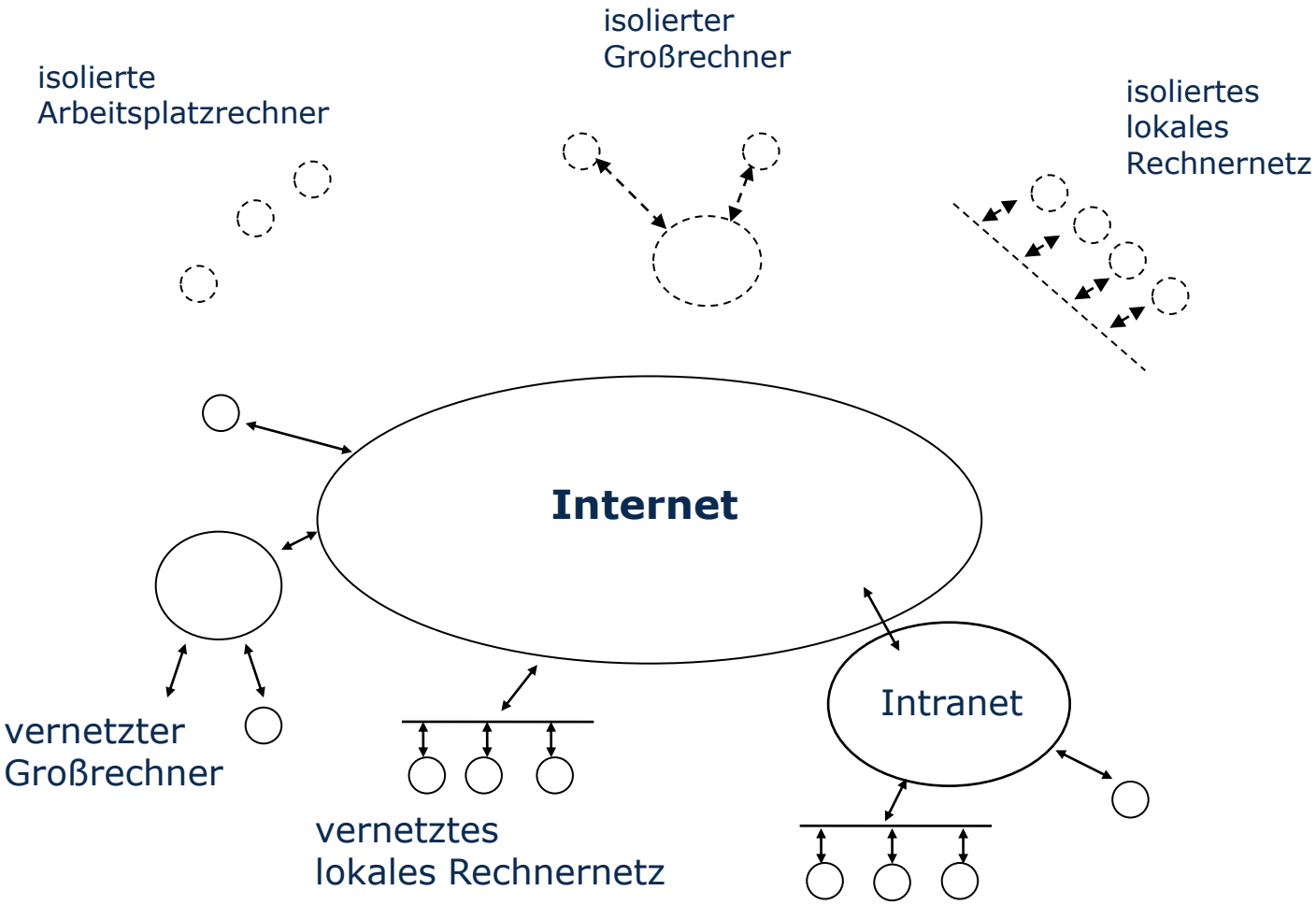
**Vermittlungsschicht**

**Sicherungs- und Bitübertragungsschicht**
**(keine speziellen Festlegungen)**

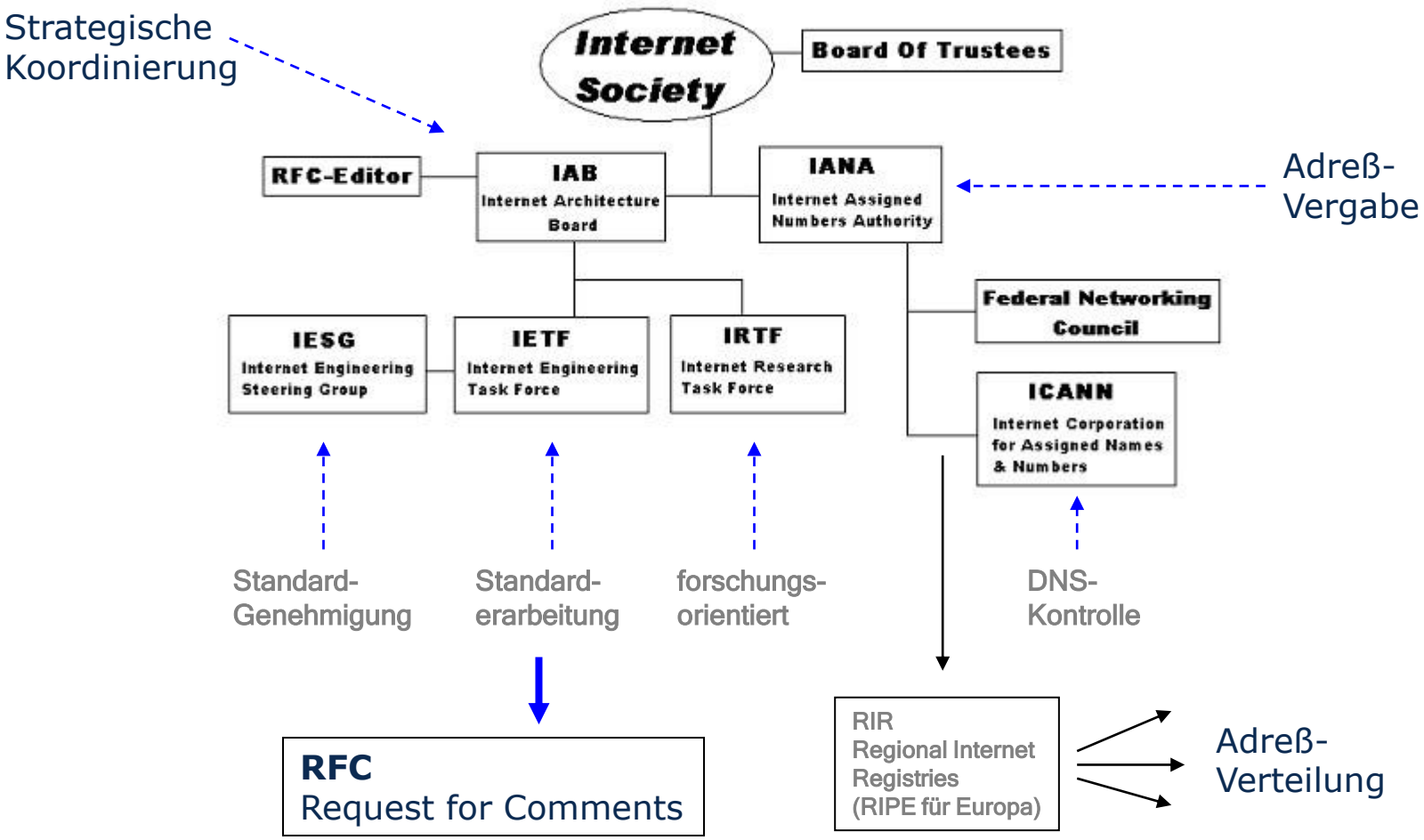
# Entwicklung des Internet

| | |
|---|---|
| 1970 | ARPANET (ca. 100 Rechnernetze), 50 kbit/s-Leitungen |
| 1973 | TCP/IP, Internetzwerk-Architektur |
| … | |
| … | |
| 1992 | WWW (World Wide Web) |
| 1995 | Neue Protokolle (IP next generation etc.) |
| 1995 | zunehmende private Nutzung |
| 1996 | zunehmende kommerzielle Nutzung |
| 1999 | zunehmende Verbreitung von Multimedia |
| 2000 | Weitere deutliche Leistungserhöhung<br>Gigabit-Wissenschaftsnetz |
| … | |
| → | „Internet der Dienste“ |

# Trend - weltweite Vernetzung über Internet



# Internet - Organisation



# RFC (Request for Comments)

**Standardisierungsstatus**

- Offene Diskussion in IETF-Arbeitsgruppen
  → Veröffentlichung als „Proposed Standard"
- Analyse/Test abgeschlossen, Modifikation noch möglich
  → „Draft Standard"
- Standard zur Nutzung freigegeben
  → „Full Standard"

**Protokollstatus**

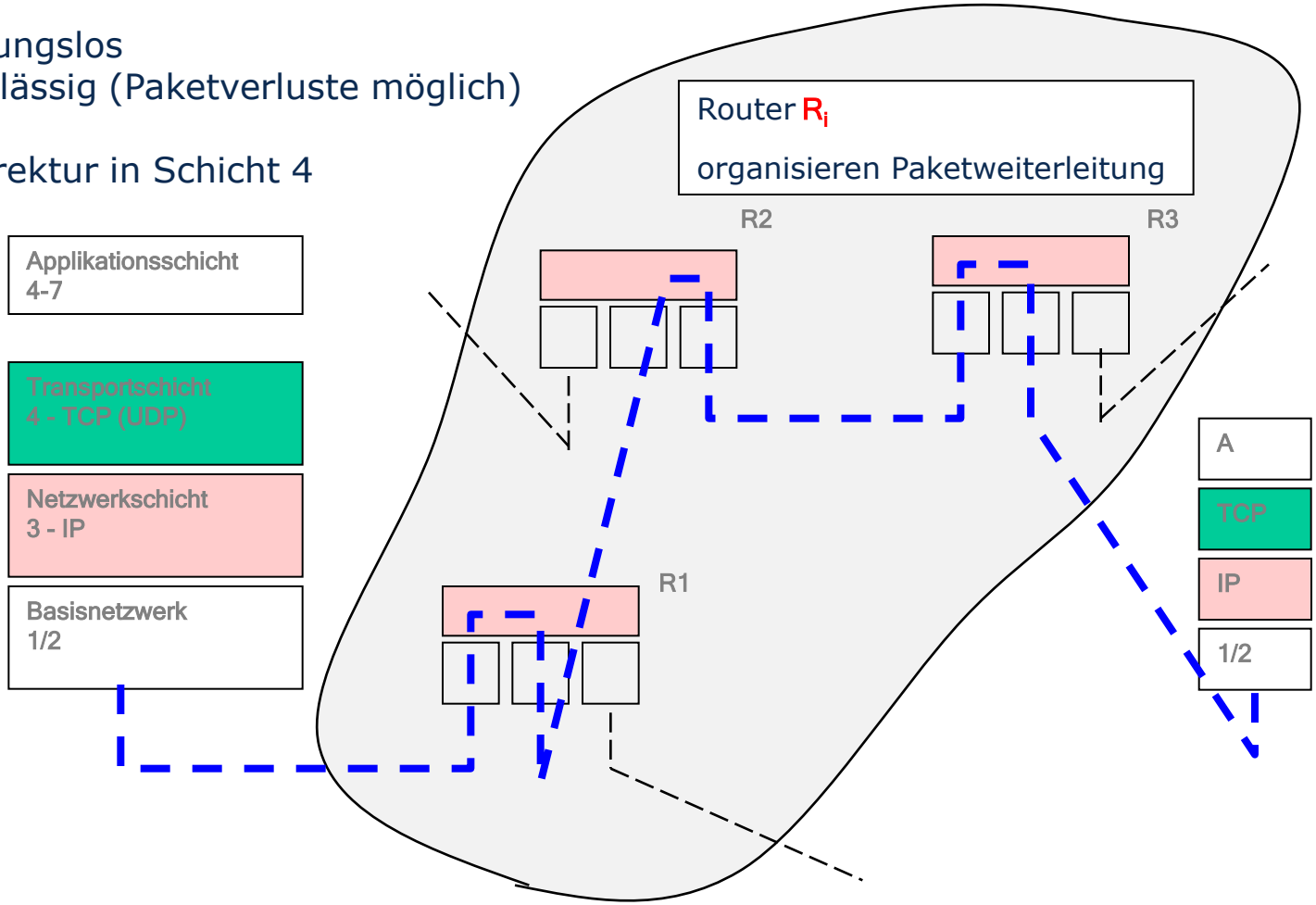
| | |
|---|---|
| • „experimental" | Testphase |
| • „informational" | Diskussion, evtl. prorietär, … |
| • „historic" | Protokoll veraltet |
| • „required" | zwingend zu verwenden |
| • „recommended" | zur Verwendung empfohlen |
| • „not recommended" | … nicht empfohlen |

# Internet - Architektur

## Vermittlungsnetz für Pakete (adressierte Informationseinheiten)

- verbindungslos
- unzuverlässig (Paketverluste möglich)

Fehlerkorrektur in Schicht 4

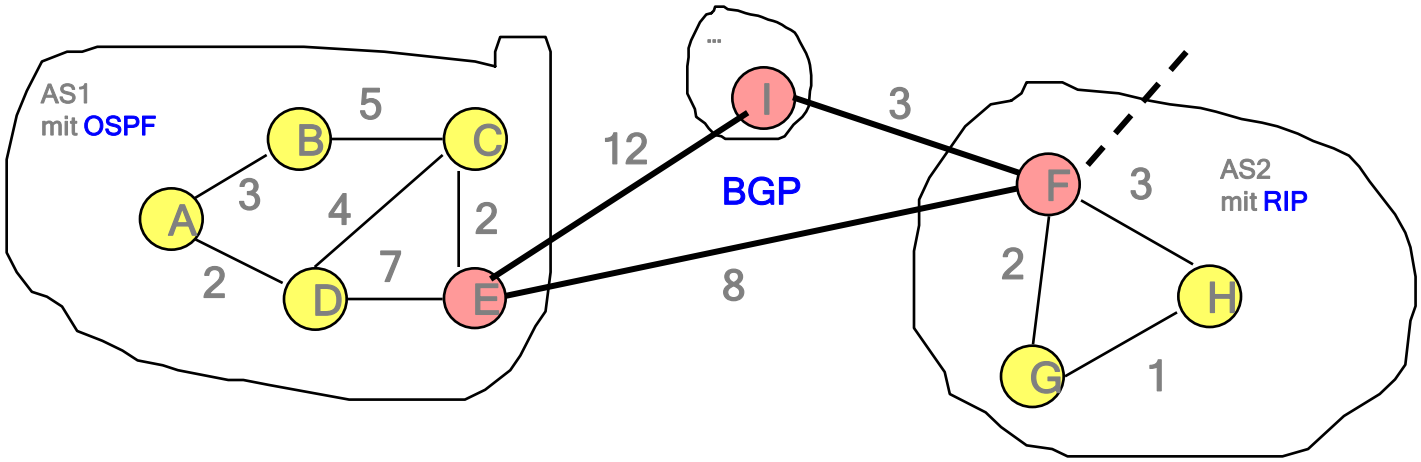


# Internet „Netz von Netzen“

Gesamtnetz-Wegewahl nur für kleinere Netze beherrschbar

→ **Unterteilung des Internet in autonome Systeme (AS)**
2008: ca 110 000 AS; Anmeldung durch Provider bei RIR`s

- AS-internes Routing
  in verschiedenen AS u.U. verschiedene Routingprotokolle
- Routing zwischen den AS
  AS-Adressierung über 16-bit-ID, neuerdings auch über 32bit-ID



# Format eines IPv4-Headers

| Bit | 1 … 4 | 5 … 7 | 8 … 15 | 16 .. 19 | 20 … 31 |
|---|---|---|---|---|---|
| | Version \| IHL | Service Typ | Gesamtlänge | | |
| | Identifikation | | Flags \| | Fragment Offset | |
| | Time To Live | Protocol | IP-Header-Prüfsumme | | |
| | IP Source Adresse | | | | |
| | IP Destination Adresse | | | | |
| | Optionen … | | Füllzeichen | | |

| | |
|---|---|
| IHL | Header Length (variabel) |
| Type of Service: | Angaben zur gewünschten Dienstqualität |
| DF | „Don´t Fragment" – Paket darf nicht zerlegt werden |
| MF | „More Fragments" – weitere Fragmente des Pakets folgen |
| Fragment Offset | Einordnung des aktuellen Fragments |
| Time to Live | Max. Lebensdauer (in Sek., in der Praxis Angabe der Hops) |
| Protocol | Angabe des Transportprotokolls |
| Header Checksum | Fehlerprüfung (nur Header, nicht ganzes Paket) |

# IP - Paketbearbeitung

**Kontrolle**

- Headerlänge
- IP-Versionsnummer
- Paketlänge
- Prüfsumme
- Lebenszeit
- Protokollidentifikation
- Adreßklasse bei Quell- und Zieladresse

**Fehlerfall?** Fehlernachricht an Partner-Router (über Protokoll ICMP)

**Korrekt?** Lebenszeit um 1 dekrementieren
Header neu berechnen (Kontrollsumme)

Paket weiterleiten (Nutzung von Routingtabellen)

# IPv4 - Adressierung

**32-Bit-Adressen** (4 Byte)

⇒ $2^{32}$ *(= 4 294 967 296)* mögliche Adressen

Vergabe durch **IANA** (Internet Assigned Numbers Authority)
an regionale Organisationen, z.B. RIPE NCC (Network Coordination Centre)
Unterverteilung durch Internetprovider

Schreibweise: byteweise dezimal durch Punkt getrennt
z.B. **141.76.40.3**

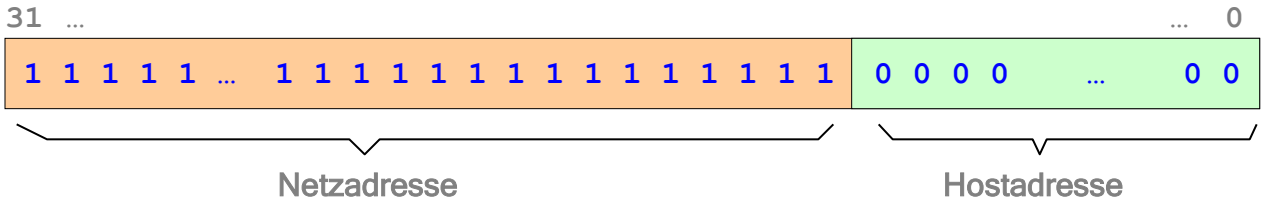
**Problem:** Adressen enthalten keine Routinginformationen
Internetrouter ← $2^{32}$ Tabelleneinträge !!!!

**Lösung:** Unterteilung IP-Adresse in Netz- und Hostadresse
Internetrouter ← nur noch ***ein*** Eintrag pro Netzwerk

Wieviel Bits sollten für Netzadresse reserviert werden ?
➔ variable Anzahl,
da große und kleine Netzwerke existieren

# IPv4 – Strukturierung in Netz- und Hostadresse


Regelung über Netzmaske z.B. 255.255.255.0
oder über
Angabe der Anzahl der Netzadress-Bits z.B. a.b.c.d/24




**Berechnung**

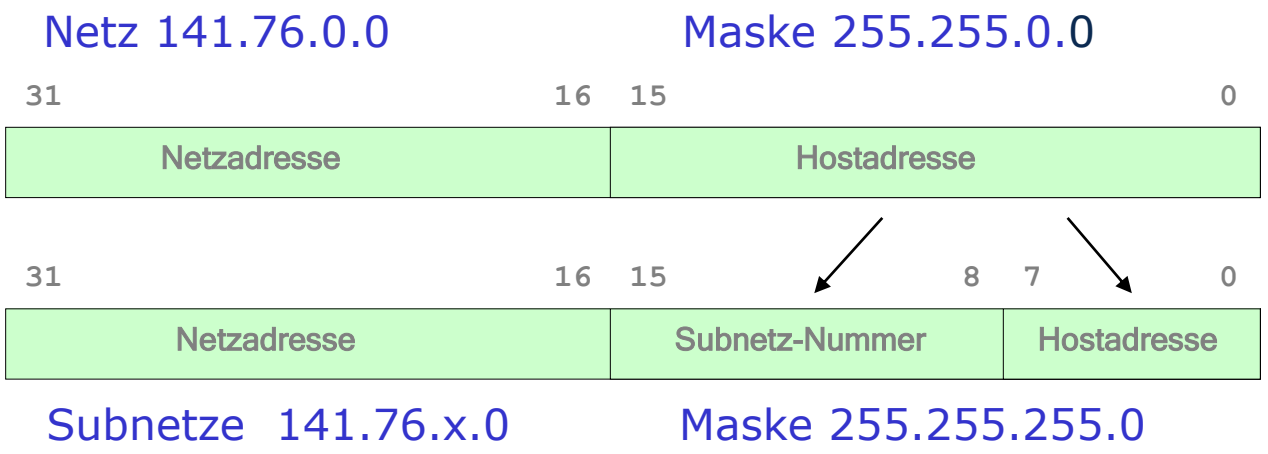
Netzadresse := IP-Adresse $\Delta$ Maske

bitweise
logische
UND-Verknüpfung

# Routing

- Routingtabelle für alle Netzadressen
- Tabelleneinträge mit IP-Adresse und Maske
- Reduktion der Tabellengrößen durch Aggregation

  z.B. nur 1 Eintrag für gesamten Verkehr zu einem Provider
- Subnetzbildung vor Ort, z.B.



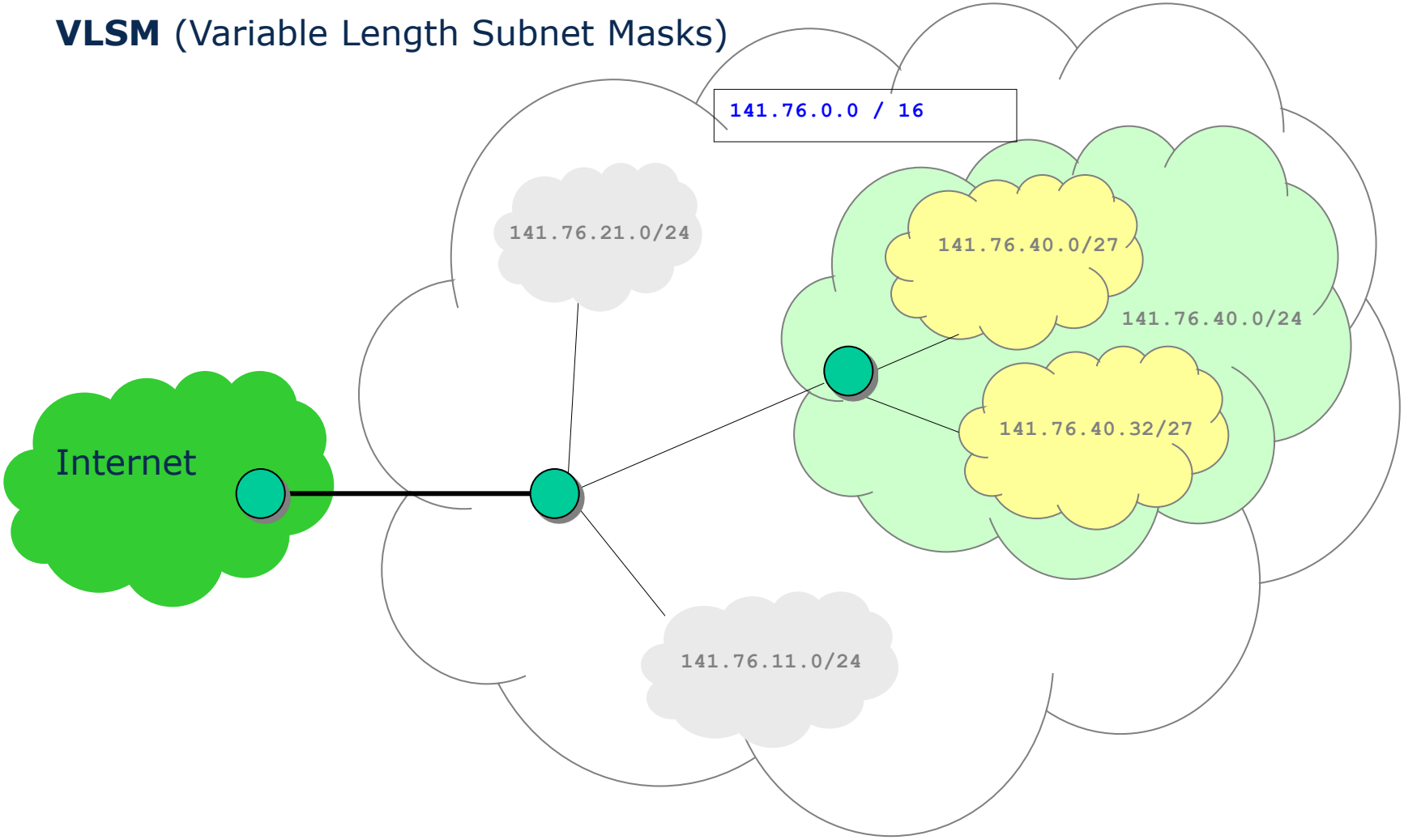
# besondere Adressen

| | |
|---|---|
| Default | 0.0.0.0 |
| Schleife | 127.0.0.1 |
| Netzadr. | alle Host-Bit=0 |
| Broadcastadr. | alle Host-Bit=1 |

| **Adreßraum reserviert für Intranet** | **Kommentar** Adressen nicht weltweit eindeutig ! |
|---|---|
| 10.0.0.0/8 | Intranetadressen können in privaten Netzen verwendet werden.<br>Im Internet werden IP-Pakete mit diesen Adressen nicht geroutet! |
| 172.16.0.0/16 | |
| 192.168.0.0/24 | |

# Subnetz - Hierarchie

**VLSM** (Variable Length Subnet Masks)



# Subnetz - Beispiel

| | Maske | |
|---|---|---|
| Base-Net | **10001101.01001100**.00000000.00000000 | 141.76.0.0/16 |
| Subnet 1 | **10001101.01001100.00101000**.00000000 | 141.76.40.0/24 |
| Subnet 1-1 | **10001101.01001100.00101000.000**00000 | 141.76.40.0/27 |
| Subnet 1-2 | **10001101.01001100.00101000.001**00000 | 141.76.40.32/27 |
| Host #1 | **10001101.01001100.00101000.001**00001 | 141.76.40.33/27 |
| Host #2 | **10001101.01001100.00101000.001**00010 | 141.76.40.34/27 |
| Host #3 | **10001101.01001100.00101000.001**00011 | 141.76.40.35/27 |
| ... | ... | ... |
| Host #29 | **10001101.01001100.00101000.001**11110 | 141.76.40.62/27 |
| Broadcast | **10001101.01001100.00101000.001**11111 | 141.76.40.63/27 |
| Subnet 1-3 | **10001101.01001100.00101000.010**00000 | 141.76.40.64/27 |
| Subnet 1-4 | **10001101.01001100.00101000.011**00000 | 141.76.40.96/27 |
| ... | ... | ... |

# ICMP (Internet Control Message Protocol)

**RFC 792** bzw. **RFC 1885** für ICMPv6

Hilfsprotokoll für den Austausch von Internetsteuernachrichten

- Fehleranzeigen (z.B. fehlerhafte IP-Pakete, Nichterrreichbarkeit, …)

  zwischen Host und Router
  zwischen Routern

- Testnachrichten
- Flußsteuernachrichten (ähnlich "Choke-Pakete")

ICMP-Daten werden als in Form von IP-Paketen übertragen


Nutzung durch IP
und spezielle Administrationsprogramme, wie *ping, traceroot, …*

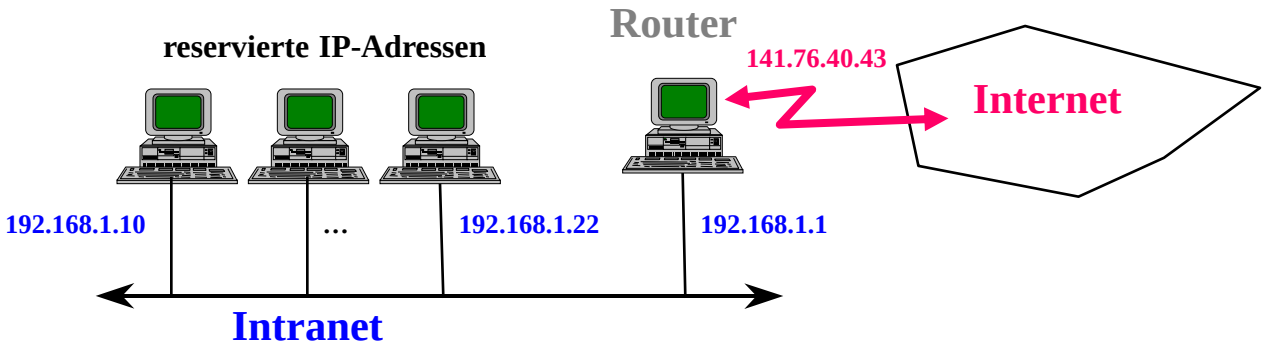
# IP – NAT/PAT (Network Address and Port Translation)

**Problem**: Internet-Anschluß für Intranet

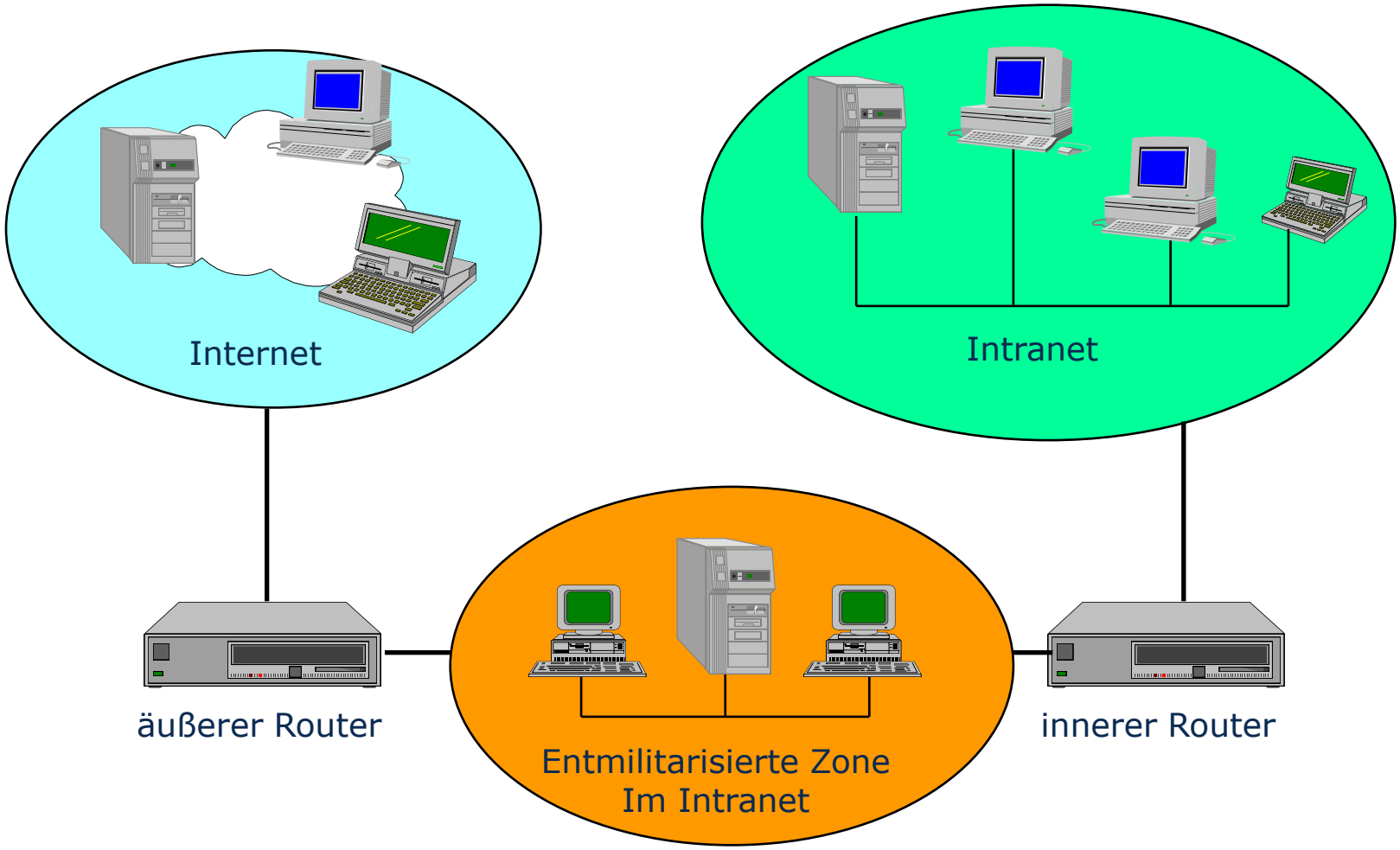
private Adressen (wegen Adreßmangel, Kosten) nicht im Internet routbar !

**Lösung:** Abbildung der Intranetadressen auf „vollwertige" IP-Adressen

- Static NAT: feste Zuordnung, z. B. 192.168.1.10 => 141.76.40.43
- Dynamic NAT: dynamische Zuordnung einer Adresse aus einem Adresspool
  → Probleme bei Verbindungsaufnahme von außen
- NAT/PAT: erweitertes Dynamic NAT
  Abbildung von Socketadressen (IP-Adresse + Port-Nummer)



# Paketfilter als Firewalls

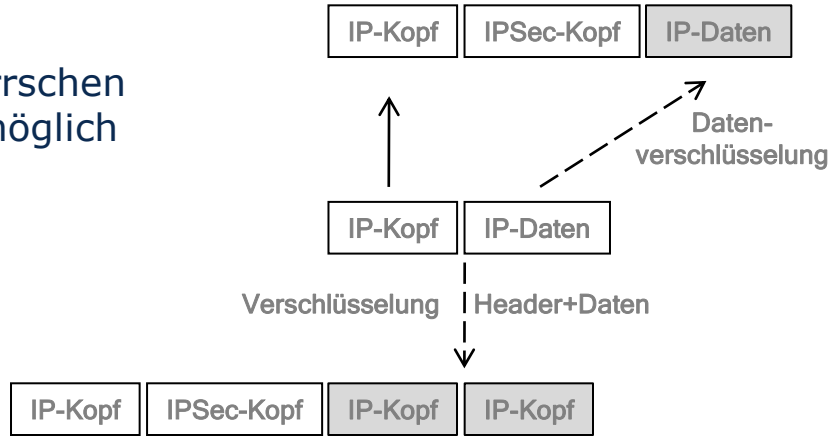


# IPSec ( IP Security )

## Transportmodus

- IP-Header mit zusätzlichem IPSec-Header
- Verschlüsselter Datenteil des IP-Pakets

→ wenig Overhead
alle Stationen müssen IPSec beherrschen
Verkehrsanalyse durch Angreifer möglich

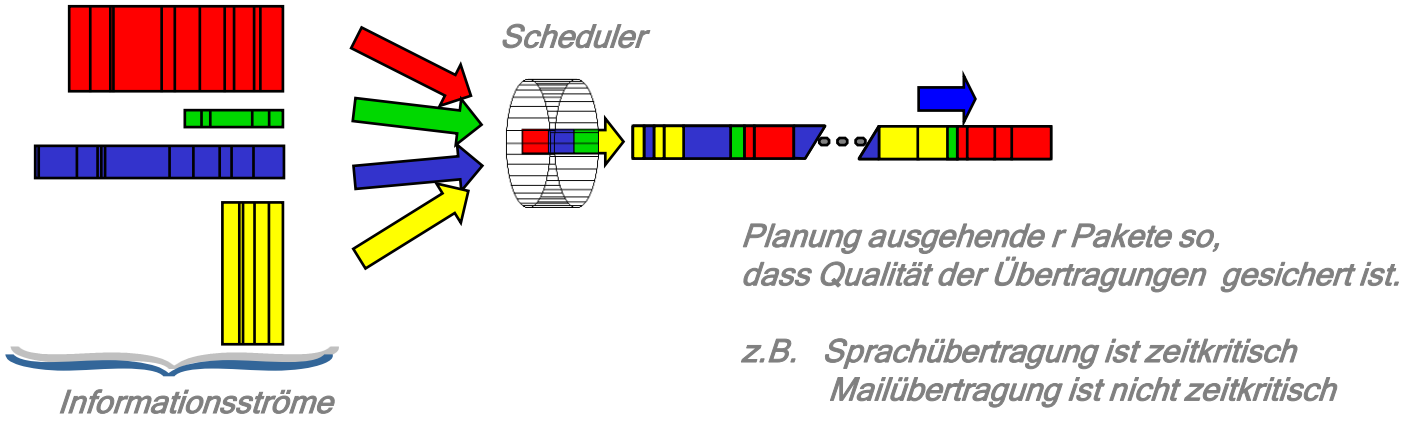



## Tunnelmodus

- IP-Paket wird komplett verschlüsselt, neuer IP- und IPSec-Header
- Verkehr über Gateway

→ Overhead größer
nur Gateway muß IPSec beherrschen
Angreifer können nur Anfangs- und Endpunkt des Tunnels feststellen

# Quality of Service (QoS) in IP-Netzwerken




Integrated Services Networks (**IntServ**)

- explizite Ressourcenreservierung entlang des Übertragungsweges (virtuelle Verbindungen)

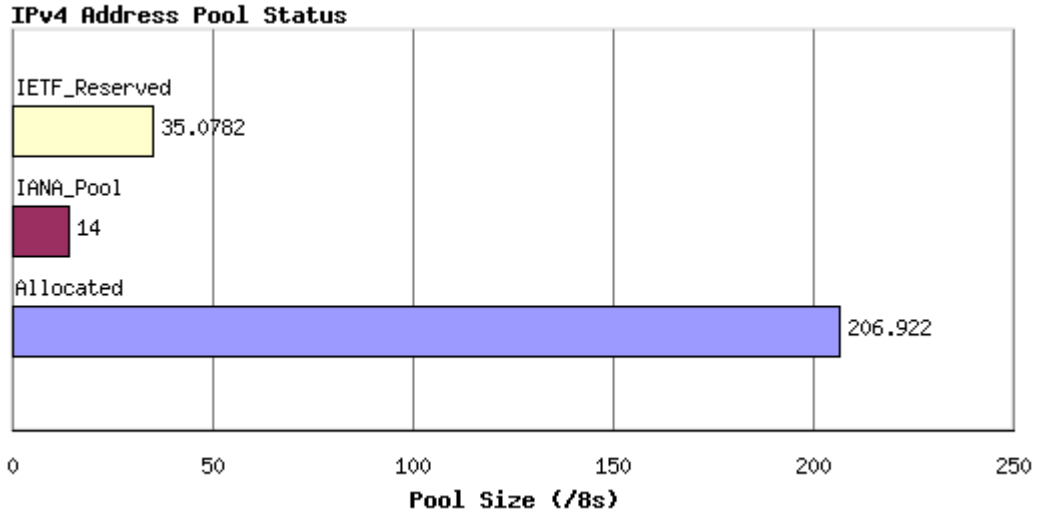
Differentiated Services Networks (**DiffServ**)

- verbindungslos, keine explizite Ressourcenreservierung, Steuerung über Angaben von Weiterleitungsprioritäten im IP-Header

# IPv4 – Adreßpool -Prognose

(http://www.potaroo.net/tools/ipv4/index.html)

IANA 4.10.2010
noch 5% Reserve an IPv4-Adressen (/8-er Blöcke)




→ Adreßpool aufgebraucht

IANA 2.6.2011
RIR 27.1.2012

# Migration IPv4 → IPv6

**Schrittweiser Übergang**

1. Implementierung in wichtigen Betriebssystemen ✓
2. isolierte IPv6-Netzwerke mit IPv4-Konvertierung zur Außenwelt ✓
3. DNS-Umstellung (Root-Server!) auf IPv4/IPv6-Doppelstack (✓)
4. Gemischter Betrieb (Kapselung von Paketen: **Tunnel**)

| | | |
|---|---|---|
| IPv6 | → IPv4 → | IPv6 |
| IPv4 | → IPv6 → | IPv4 |
| IPv4 | → … → | IPv6 |
| IPv6 | → … → | IPv4 |

5. Einstellung der Unterstützung für IPv4-Netzwerke

# IPv6

1996… IETF **RFC 2460** → IPv6 oder IPnG (IP Next Generation)
(diverse Modifikationen erschweren Akzeptanz)

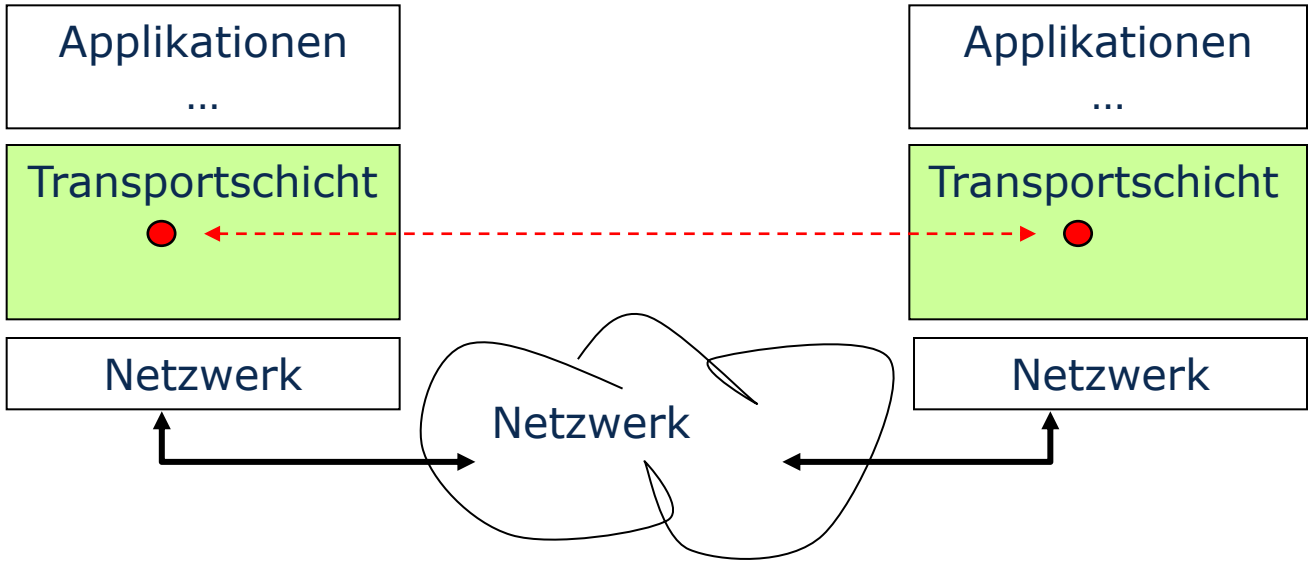
Grund Adreßmangel, Unübersichtlichkeit von IPv4 (IP, IPsec, mobile IP, …)

**Eigenschaften**

- Verwendung von strukturierten **128-Bit-Adressen** (16 Byte)
  verschiedene Adreß-Typen, Rückwärtskompatibilität zu IPv4
- Flexibles Header-Format
  (40 Byte, bessere Notation von QOS-Parametern)
- Optionen zur
  Verschlüsselung, Authentisierung, Prüfung der Datenintegrität
- Autokonfiguration
- …

# Aufgaben der Internet-Transportschicht

- Entlastung der Anwendungsprozesse von Übertragungsproblemen
- globale Adressierung der Applikationsprozesse




- 2 Transportprotokolle

UDP – verbindungslos, geringe Dienstqualität (wie IP)
TCP – verbindungsorientiert, hohe Dienstqualität

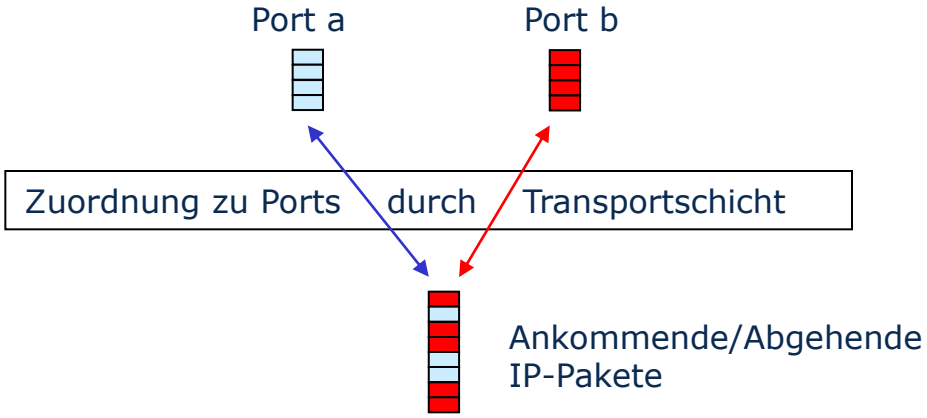
# Adressierung bei Internet-Transportprotokollen

**Socketadresse**

Rechner wird adressiert über IP-Adresse
Prozeß wird adressiert über Ports

**Port** := Nachrichtenübergabestelle auf einem Rechner
dargestellt als 16-Bit-Zahl
(TCP-Ports unabhängig von UDP-Ports)

entspricht einer speziellen Mailbox
zur Kommunikation zwischen Nutzer und Transportschicht



# Socketschnittstelle

Programmierung von Anwendungen auf Basis der Socket-Schnittstelle wird von den meisten Entwicklungsumgebungen (Compiler, …) unterstützt.

- Satz einfacher Zugriffsfunktionen
- bidirektionale Übertragung
- Zugriff auf Netzwerk ähnlich wie Zugriff auf Dateien

**Client-/Server-Kommunikation**

Server wartet

Client ergreift Initiative → Serverport muß bekannt sein
→ Client-Port frei wählbar

| Applikationsprotokoll | Transportprotokoll | Serverport |
|---|---|---|
| SMTP | TCP | 25 |
| DNS | UDP,TCP | 53 |
| HTTP | TCP | 80 |

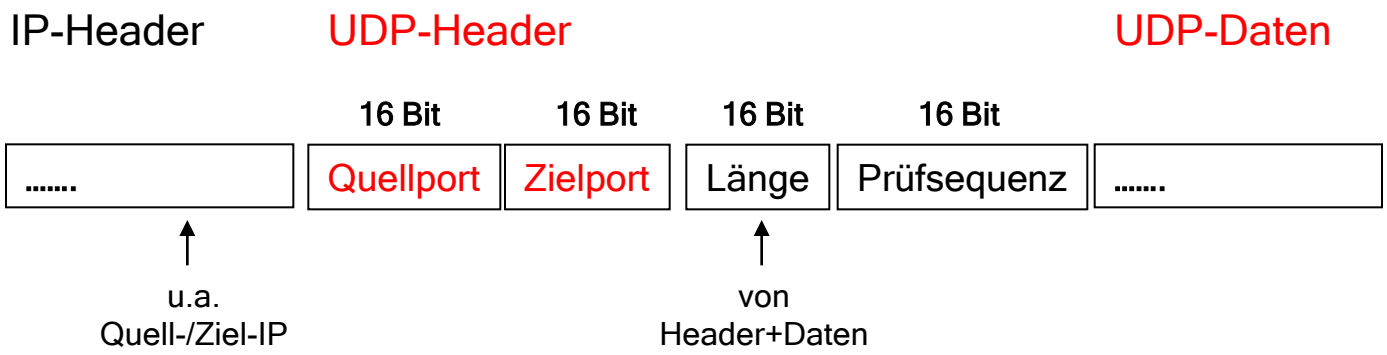
# UDP (User Datagram Protocol)

**RFC 768**

Transportprotokoll,
verbindungslos, keine Fehlerkorrektur, keine Flußsteuerung

→ geringer Overhead
→ keine Verzögerung durch Verbindungsaufbau
→ Betriebssystembelastung gering
→ geringe Zuverlässigkeit

UDP-Protokoll-Dateneinheiten werden als IP-Pakete versendet.



# TCP (Transmission Control Protocol)

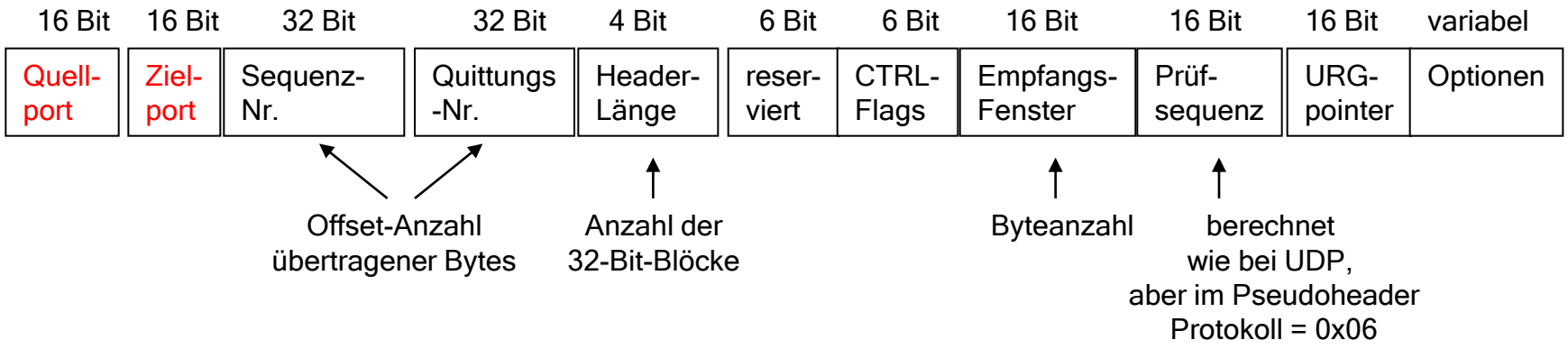
**RFC 793**

Transportprotokoll,
verbindungsorientiert, Fehlerkorrektur, Flußsteuerung

→ hoher Overhead
→ hohe Zuverlässigkeit

Protokoll-Dateneinheiten (TCP-Segmente) werden als IP-Pakete versendet.

Segment-Header



# TCP – Datenübertragung

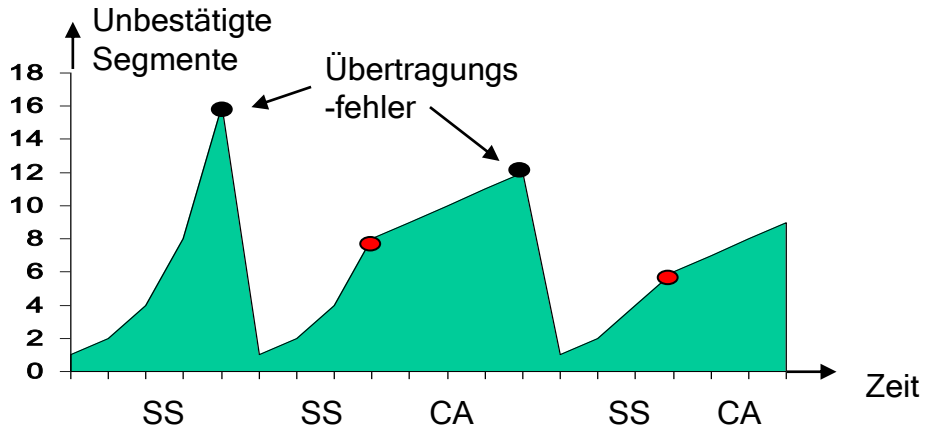
TCP behandelt Datenübertragungen ähnlich wie Ein-/Ausgaben bei Dateien

- physische Blockung der Daten ist transparent
- Segmente werden quittiert, im Fehlerfall Übertragungswiederholung

- Flußsteuerung

  Vermeidung von Überlastsituationen, faire Ressourcennutzung

  Datenrate  exponentieller Anstieg bei Slow Start (SS)
  linearer Anstieg bei Congestion Avoidance (CA)



# Domain Name System (DNS)

Namen benutzerfreundliche Bezeichner für Computer im Internet
lange Gültigkeitsdauer

ICANN Organisation der Namensvergabe

Namensraum - hierarchische Baumstruktur

| | | |
|---|---|---|
| • root | | |
| • top level domain | z.B. | de |
| • domain | | tu-dresden |
| • sub level domain | | inf |
| • host name | | mephisto |

Schreibweise von rechts nach links, getrennt durch „.“

mephisto.inf.tu-dresden.de

**DNS** organisiert im laufenden Betrieb Zuordnung von

Internetname ← → IP-Adresse

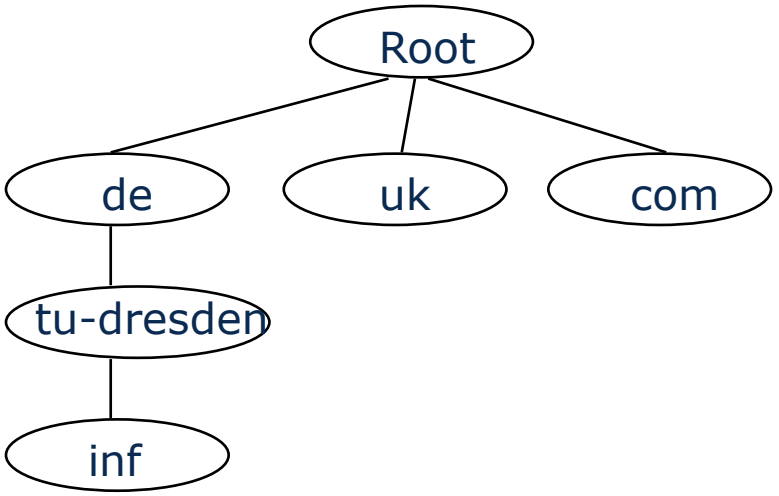
# DNS – Domänenstruktur

applikationsoriente Namen

| | |
|---|---|
| traditionell (US-orientiert): | com, firm, edu, gov, mil, net, org, tv |
| neu: | biz, info, pro, name, aero, museum, coop |

Staaten-Identifikationen

de, uk, de, fr, nl, cz, pl, eu, ua

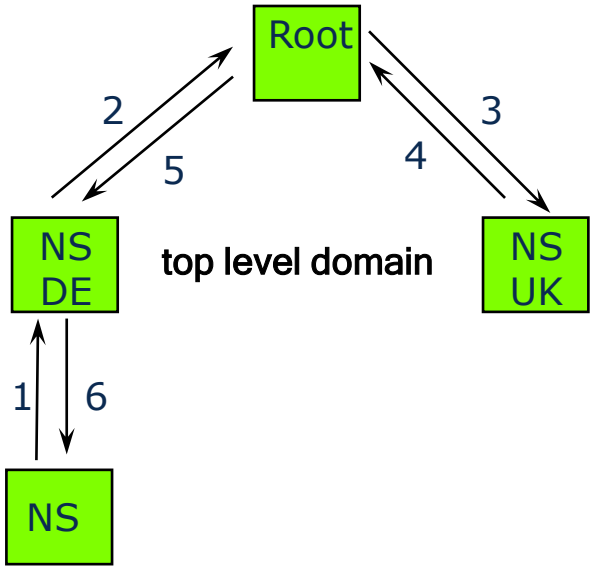



**Vergabe der domain-Namen**
und der sub-level-domain-Namen

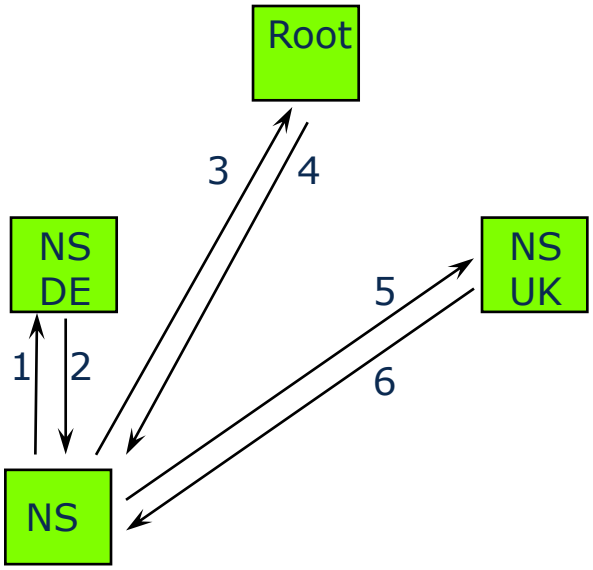
durch untergeordnete
NIC (Network Information Center)
z.B. DENIC

# Anfrageauflösung - verteiltes Nameserversystem

Anwenderrechner muss mindestens 1 Nameserver kennen.
Nameserver verwalten jeweils einen Teil des gesamten Adressraumes.




Rekursive Anfrage




iterative Anfrage

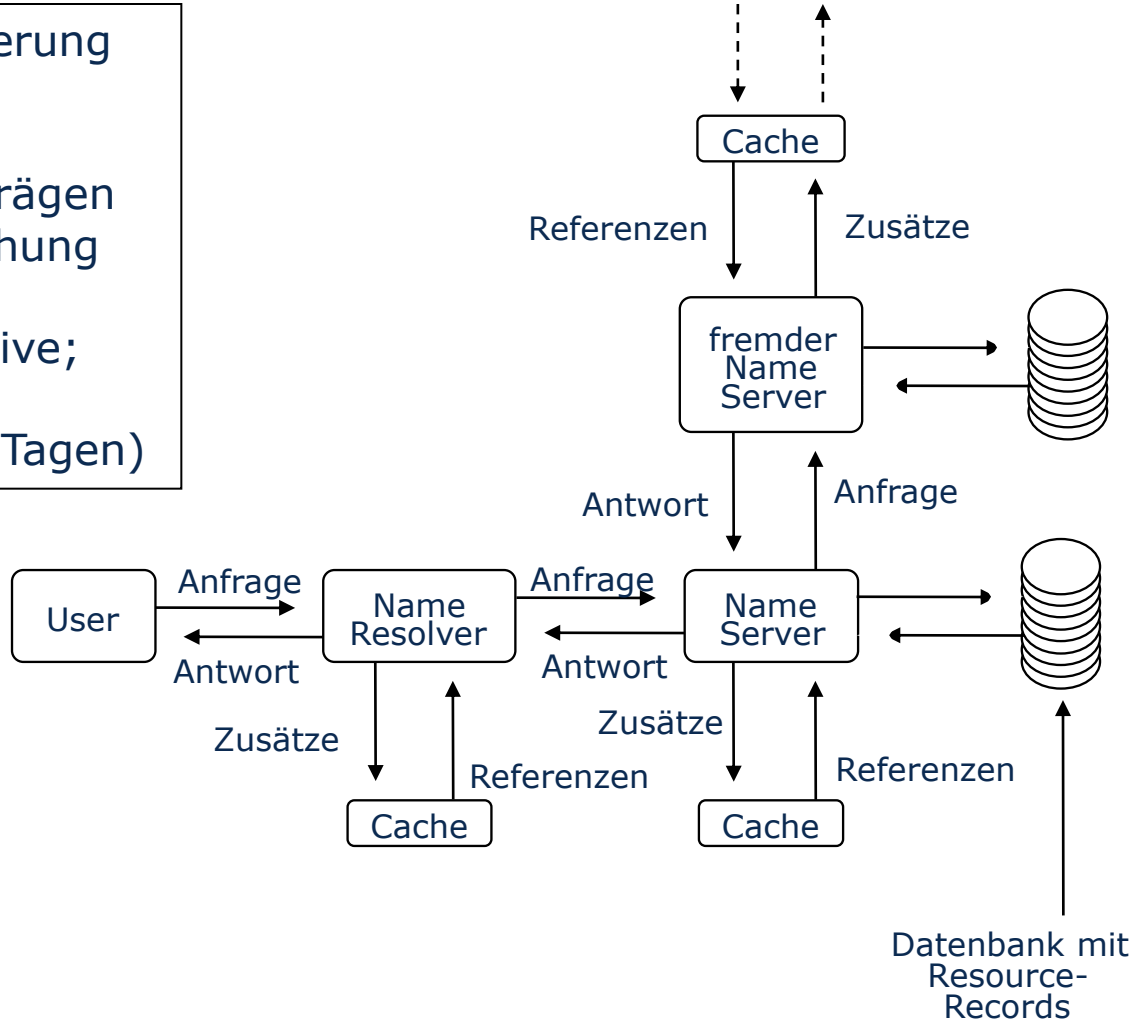
Beispiel: Welche IP-Adresse hat der Rechner mit dem „www.vodafone.uk“ ?

# DNS – Abfrage

Effizienzverbesserung

**Caching**
von Namenseinträgen
mit Zeitüberwachung

(TTL – Time to Live;
Bereich
von Minuten bis Tagen)



# DNS – Root Server

RFC 1035