

Rechnernetze: (2) Infrastruktur



Prof. Dr. Klaus-Peter Kossakowski



Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell
- Netzwerk als Infrastruktur
 - Adressierung, DNS und andere Details
 - Entwicklung im Internet
- Layer 7: Anwendungsschicht
- Layer 7/4: Socketprogrammierung
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
- Layer 2: Sicherungsschicht



Inhalte dieses Kapitels

In diesem Kapitel betrachten wir einige Details des Internet-Modell noch etwas genauer und vertiefen das Verständnis der Schichten und Schichtung.

Danach gewinnen wir einen Überblick über die Adressierung im Internet und die Namensauflösung mit DNS.

Schließlich gehen wir noch kurz auf den – auf den ersten Blick etwas seltsam anmutenden – Entwicklungs- und Standardisierungsprozess im Internet ein.



Ziele dieses Kapitels

Sie können das Internet-Modell und seine Schichten richtig benennen und die Funktionen der einzelnen Schichten gegeneinander abgrenzen.

Sie können die Verwendung von IP-Adressen erklären, insbesondere das Sub-Netting und den Einsatz der Netmask.

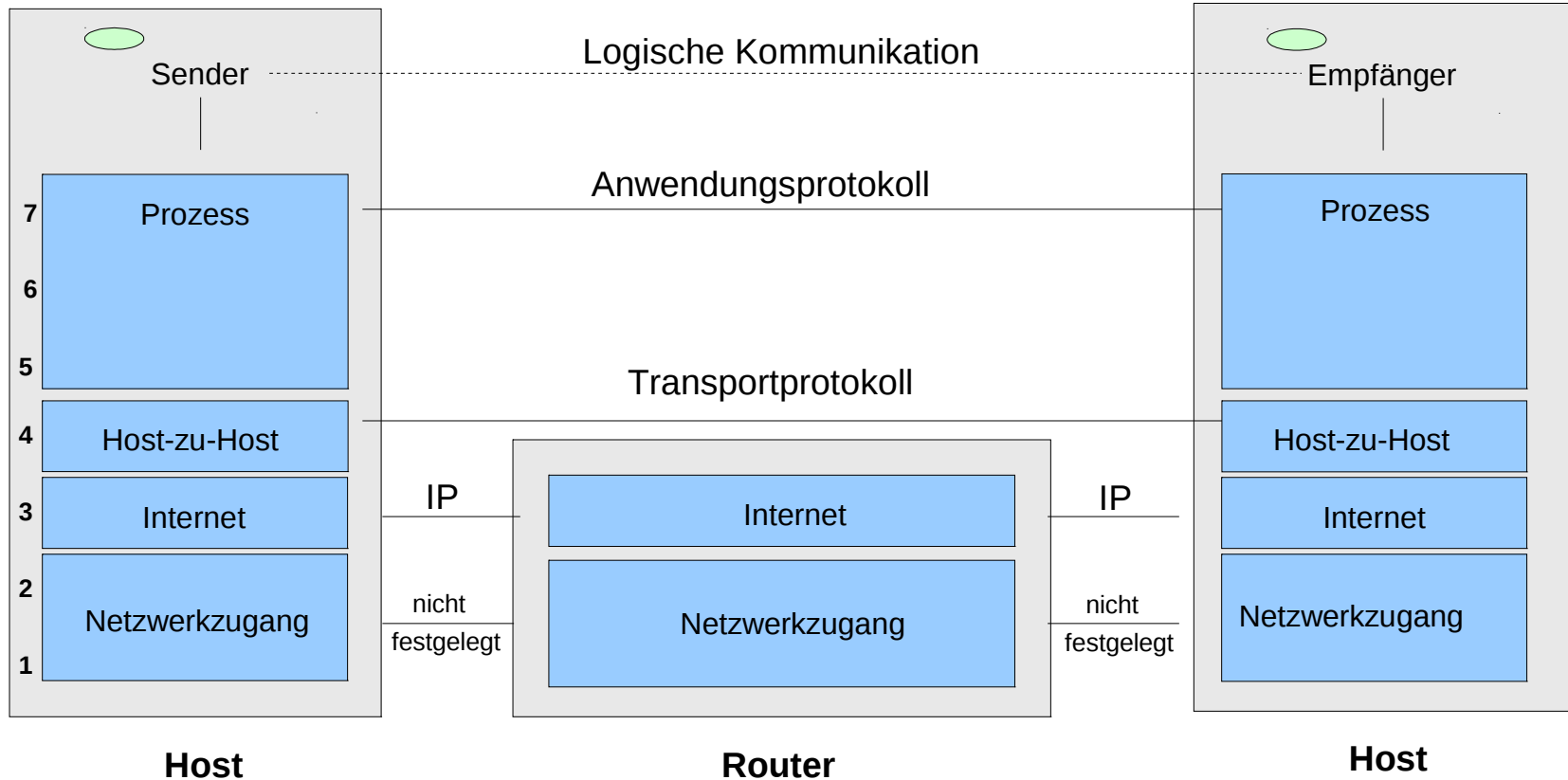
Sie können die Namensauflösung innerhalb des DNS-Systems erklären, die Aufteilung des Namensraums im Internet darstellen und die beteiligten Komponenten benennen und erläutern.



Das Internet-Modell



Das Internet-Modell





Das Internet-Modell

■ Process:

Implementiert durch Anwendungs- und Dienstprogramme

■ Host-to-Host:

Bietet die Ablaufumgebung für kommunizierende Prozesse

■ Internet:

Ermöglicht die Übertragung von Paketen zwischen Rechnern a.k.a. Hosts

■ Network Access:

Stellt Zugriff auf Übertragungsmedien bereit



Process Layer

Ergänzungen des Betriebssystems realisieren die – für Benutzer interessanten – Anwendungen und sprechen die Transportschicht an!

Es gibt dementsprechend eine Unzahl von sehr spezifischen Protokolle mit ebenfalls spezifischen Clients, z.B.:

- FTP, Telnet, SMTP (klassisch)
- DNS, RIP, SNMP (administrativ)
- HTTP, IRC, SIP (Internet)
- SQL*net, BitTorrent (spezifisch)



Host-to-Host Layer

Als Bestandteil des Betriebssystems ermöglicht die Transportschicht die Kommunikation von Programmen

- **User Datagram Protocol (UDP) bietet einen ungesicherten, verbindungslosen Übertragungsdienst**
- **Transmission Control Protocol (TCP) liefert einen gesicherten, verbindungsorientierten Übertragungsdienst**
- **Weitere Transportprotokolle für andere Anwendungsklassen**



Internet Layer

Als Bestandteil des Betriebssystems ermöglicht diese die Basiskommunikation von Rechner zu Rechner = Paketaustausch!

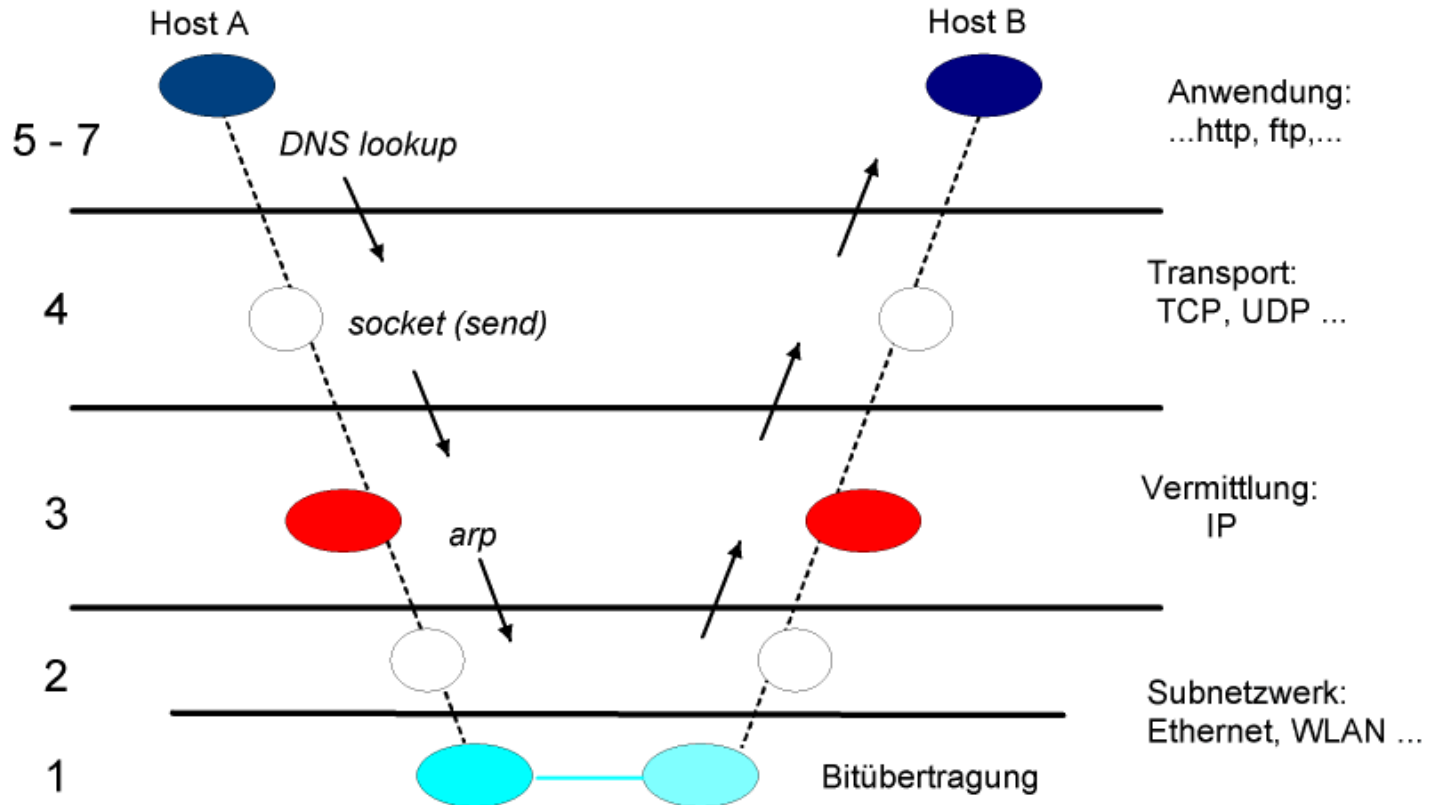
- **Liefert mit dem Internet Protocol (IP) einen ungesicherten, verbindungslosen Übertragungsdienst**
- **Weitere Protokolle:**
 - ICMP (Kontrollprotokoll)
 - IGMP (Internet Gruppenmanagement)
 - ARP/RARP (Adressauflösung)
 - BGP/EGP/OSPF (Wegfindung)



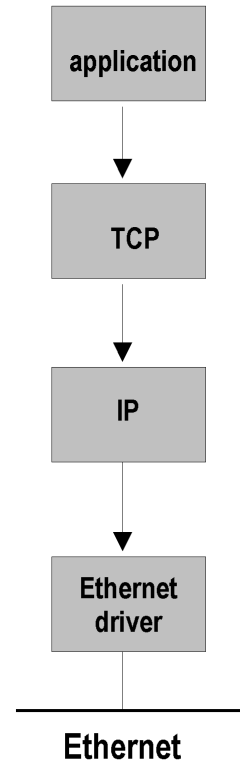
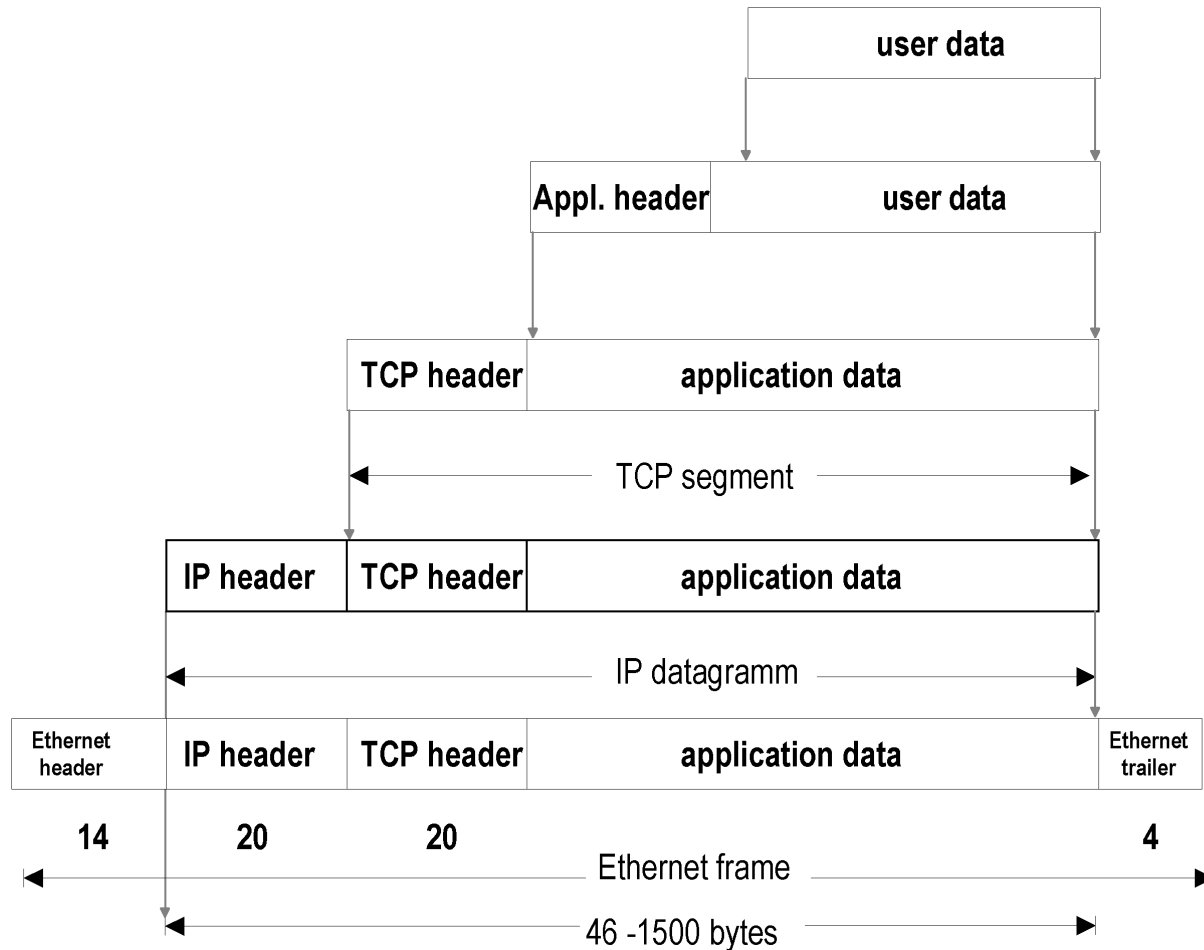
Weitere wichtige Begriffe

- Netzwerke verbinden Hosts untereinander
- Gateways oder Router verbinden Netzwerke miteinander
- Ports dienen ergänzend zu IP-Adressen zum Zugriff auf Dienste
 - Dienste verwenden sogenannte well-known Ports (80/tcp für HTTP, 123/udp für NTP)
- Hostnames (=Rechnernamen) verbergen die numerischen IP-Adressen vor den Augen der Benutzer

Das „V“ der Kommunikation



Jedem Protokoll seinen Header





Wer kennt schon 127.0.0.1?



Adressierung im Internet

■ Allgemeine Anforderungen

- Kompakt
- Universell – egal welches System

■ Hardware

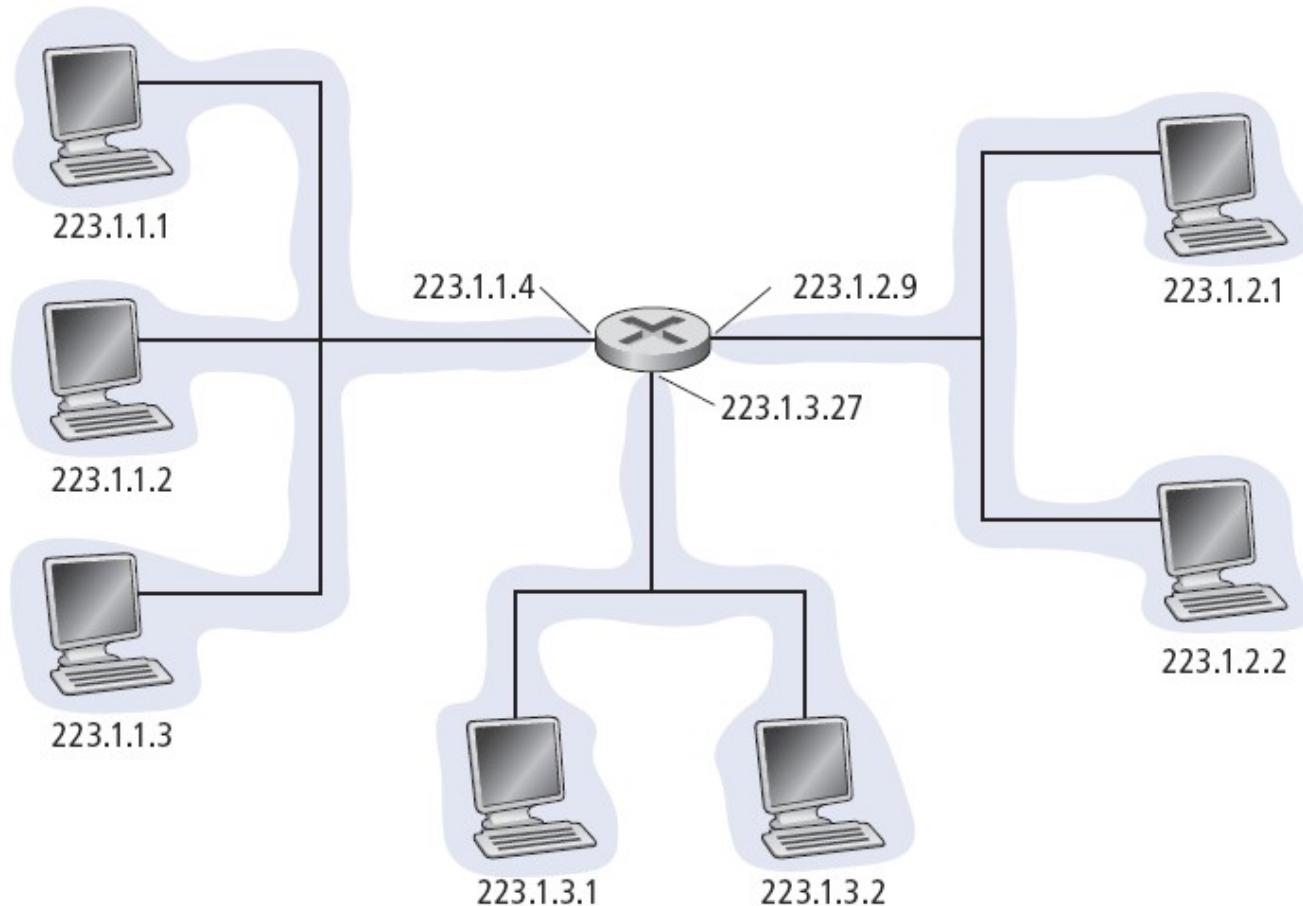
- unabhängig, also logische Adressierung

■ Routing

- Unterstützung einer effizienten Wegfindung
- Dezentral



Und wie sieht das aus?





Adressierung im Internet

- **IPv4-Adresse:**

32-bit Identifier für Host- und Router-Interface

- **Interface:**

Schnittstelle zwischen Host/Router und physikalischer Verbindungsleitung

- Router haben viele Interfaces
- Hosts können mehrere Interfaces haben
- IP-Adressen werden einem Interface – nicht einem Host oder Router – zugewiesen

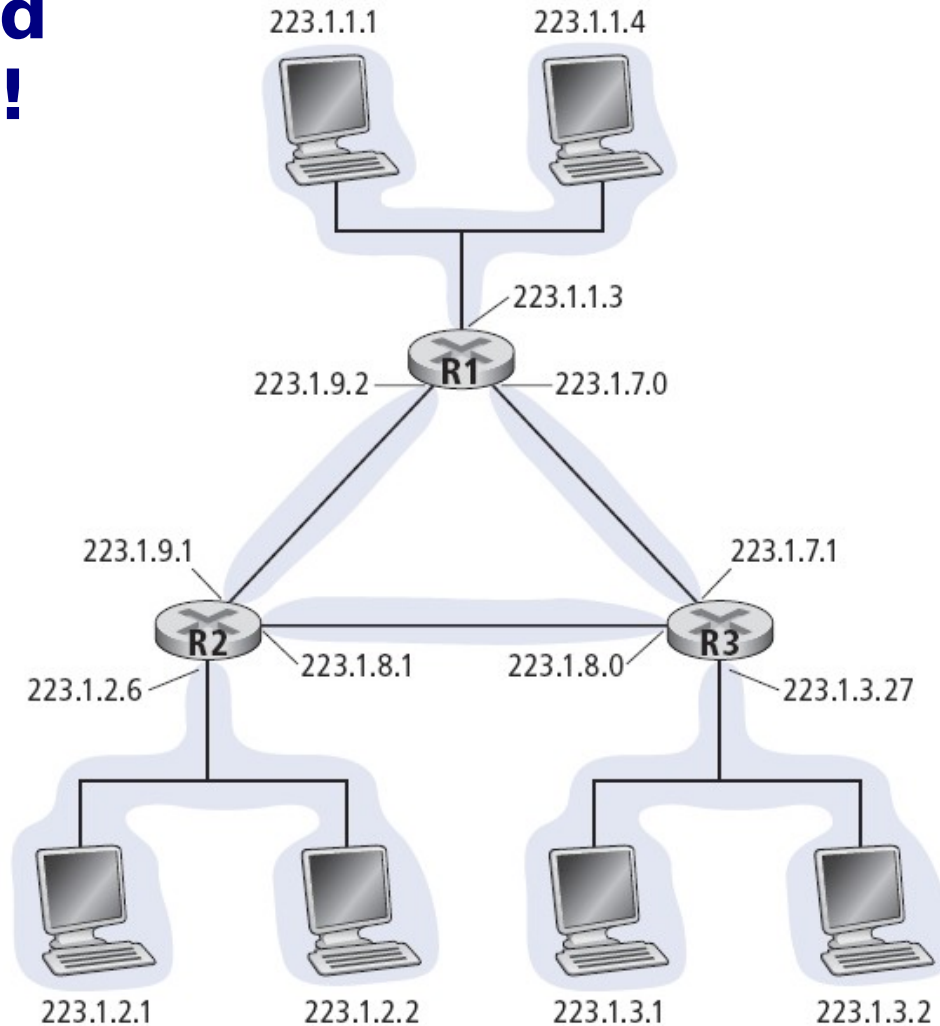


Adressierung im Internet (2)

■ Netzwerk aus Sicht des IP-Protokolls

- Alle Interfaces, die sich physikalisch gegenseitig ohne Inanspruchnahme eines Routers erreichen können
- Diese Interfaces erhalten jeweils IP-Adressen mit einem identischem Anteil, der sogenannten Netzwerk-Adresse

Und es wird komplexer!

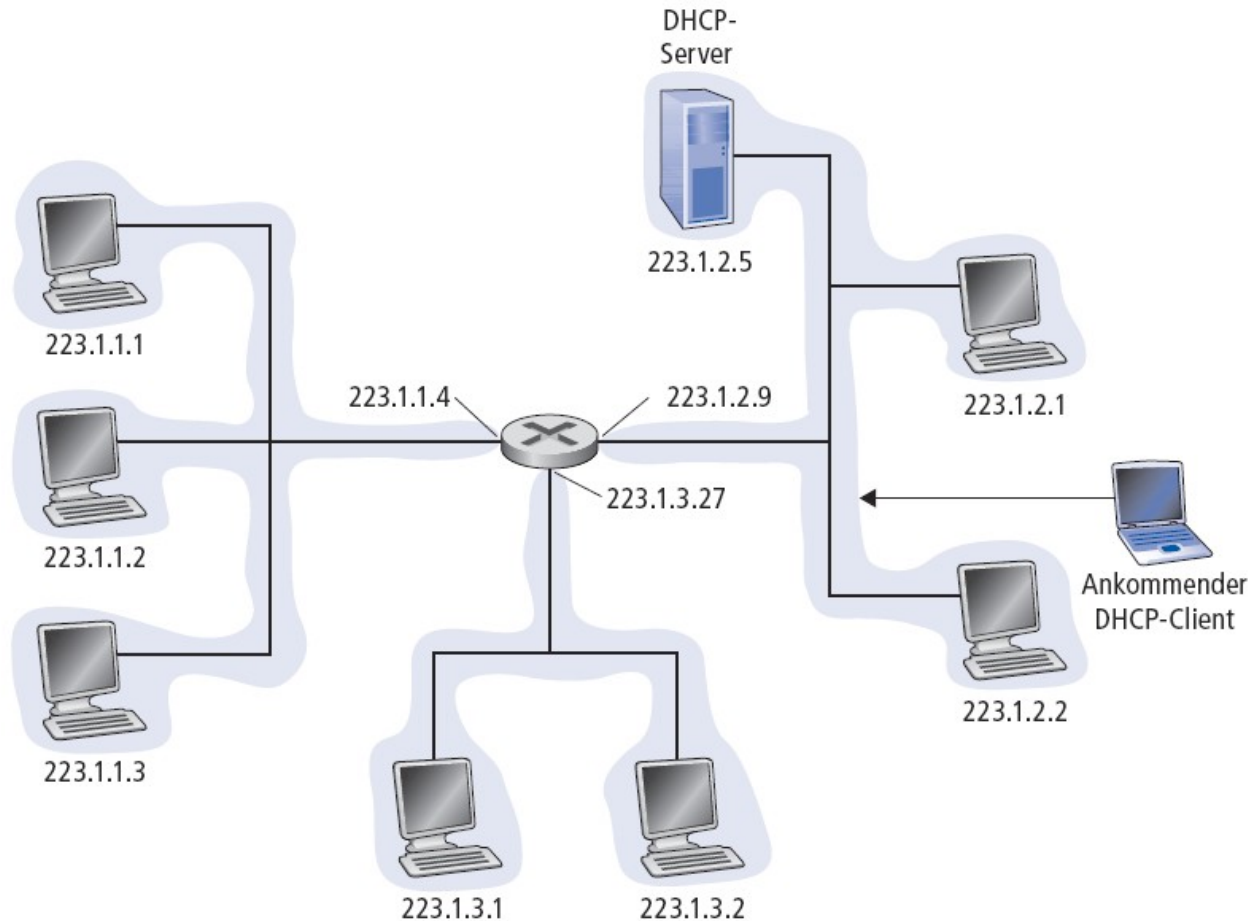




Zuweisung von IP-Adressen

- Eintrag in eine Systemdatei (von Hand durch Administrator)
- Per Dynamic Host Configuration Protocol [DHCP, RFC 2131]
- Möglichkeiten der Zuordnung
Host – IP-Adresse:
 - Statisch (z.B. in Firmennetzen) mit “fester” Zuordnung (über LAN-Adresse)
 - Dynamisch (z.B. bei ISPs) mit “zufälliger” Zuordnung der IP-Adresse aus einem Pool

Einfacher ist es mit DHCP





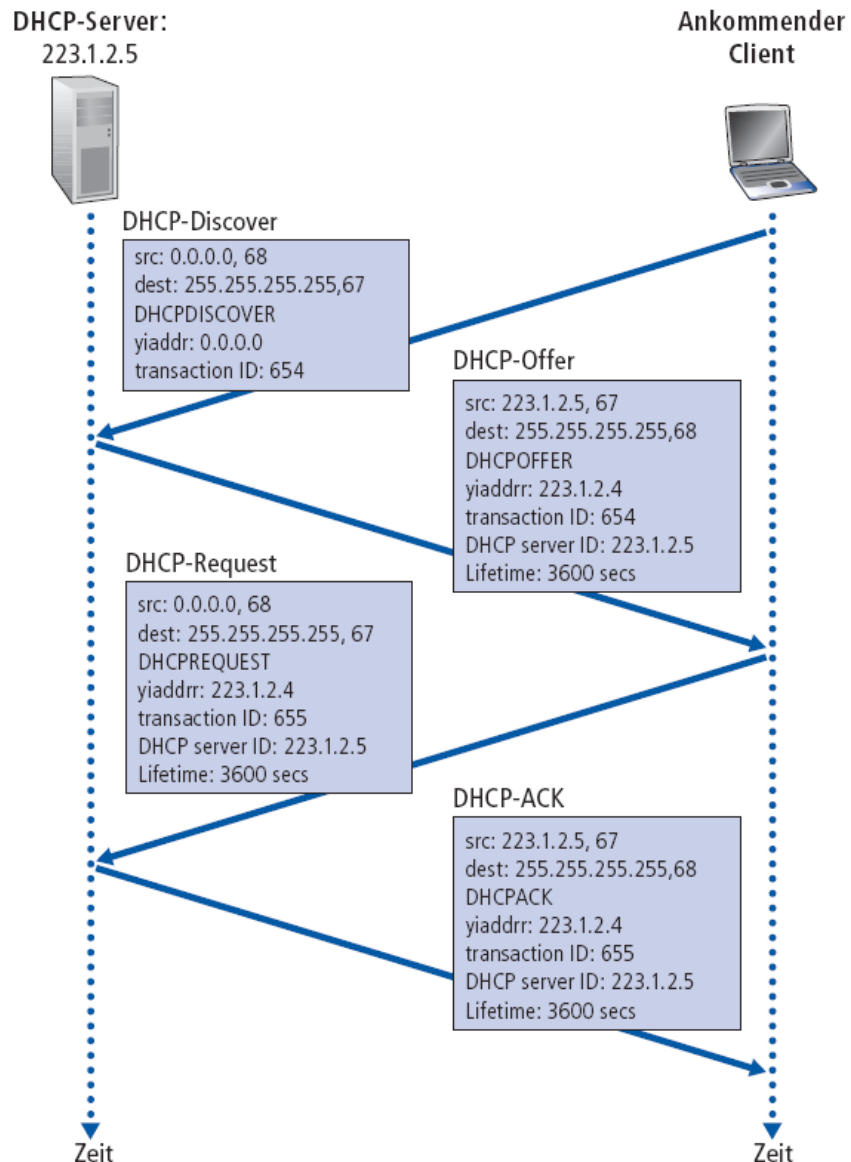
Zuweisung von IP-Adressen (2)

■ Per DHCP dynamische Adresszuweisung als “plug-and-play”

■ Protokollablauf

1. Host sendet “DHCP-Discover” als Broadcast-UDP-Message
 - IP-Zieladresse: 255.255.255.255
 - Quelladresse: 0.0.0.0
2. DHCP-Server antwortet mit “DHCP-Offer”
 - Broadcast oder LAN-Adresse aus Schicht 2
3. Host fragt nach IP-Adresse: “DHCP-Request”
4. DHCP-Server sendet IP-Adresse: “DHCP-Ack”

DHCP als Protokoll





Klassische Struktur von IP-Adressen

Diese müssen in einem abgegrenzten Kommunikationssystem eindeutig sein.

Sie sind hierarchisch geordnet und teilen sich in eine Netzwerk- und eine Rechneradresse auf, wodurch Netzwerkstrukturen gebildet werden können.

Klasse	Beschreibung	Bit 0	Bit 1	Bit 2	Bit 3
A	Wenige Netzwerke, viele Rechner	0	*	*	*
B	Mittlere Verteilung von Netzwerken und	1	0	*	*
C	Viele Netzwerke, wenige Rechner	1	1	0	*
D	Multicast-Adressen	1	1	1	0
E	Nicht definiert	1	1	1	1

* ::= { 0, 1 }

IP-Adressen: Klassen



Klasse A

0	Netzwerkadresse							Hostadresse																							
0	1	0	1	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0								
5				9				8				1				0				1				8				2			
89								129								1								130							

Klasse B

1	0	Netzwerkadresse												Hostadresse																	
1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	
8				0				0				5				0				1				8				2			
128								5								1								130							

Klasse C

1	1	0	Netzwerkadresse															Hostadresse																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																				
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

IP-Adressen: Klassen (2)



Klasse D

1	1	1	0	28 Bit Multicast Adresse
---	---	---	---	--------------------------

Klasse E

1	1	1	1	0	27 Bit reserviert
---	---	---	---	---	-------------------

Netzadressen und zugehörige Adressklassen:

Netzklasse	Wert
A	0 - 127
B	128 - 191
C	192 - 223
D	224 - 239



IP-Adressmasken (Netmasks)

- Jeder Rechner benötigt eine eindeutige hostspezifische IP-Adresse
- Jeder Rechner muss aber auch wissen, in welchem Netz er diese IP-Adresse hat
- Die „netmask“ ist eine Maskierung der Net-Adresse
 - Die Maske trägt eine Eins an jeder Bitposition, die einem Netzwerkbit und eine Null an jeder Position, die der Hostadresse entspricht.



IP-Adressmasken (Netmasks, 2)

- Die „netmask“ ist eine Maskierung der Net-Adresse
 - Die Maske trägt Einsen an jeder Bitposition, die einem Netzwerkbit entspricht
 - Und eine Null an jeder Position, die der Hostadresse zugeordnet ist.

Klasse	Maske - binär	Maske - dezimal
A	1 1 1 1 1 1 1 1 0	255.0.0.0
B	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	255.255.0.0
C	1 0 0 0 0 0 0 0 0	255.255.255.0



IP-Adressmasken (Netmasks, 3)

Für jedes Bit der IP-Adresse führt das Gerät eine logische UND Verknüpfung durch.

■ Beispiel:

Host hat IP-Adresse 172.21.35.17

Netmask ist 255.255.0.0

binäre Darstellung																dezimal
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	1	= 172.21.35.17
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	= 255.255.0.0
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	1	= 172.21.0.0



IP-Adressen mit Besonderheiten

- **Klasse A Adresse mit der Nummer 127 ist für die Loopback-Funktion reserviert**
- **Der Wert 255 in einem Oktett entspricht der Broadcast-Adresse und ist reserviert**
 - 126.255.255.255 spricht alle Rechner im Netz 126 an
 - 255.255.255.255 adressiert alle Rechner in allen Netzen



IP-Adressen mit Besonderheiten (2)

0 Adressen:

- Früher bezeichnete der Wert „0“ als Broadcast-Adresse alle Rechner im Internet
- Heute nicht mehr offiziell genutzt
 - Aber evtl. kennt ein Rechner die noch ;)



IP-Adressen mit Besonderheiten (3)

Private IP-Adressen:

- Erweiterung des verfügbaren Adressraumes
- Sicherheitsgründe
- Kostengründe

Netzadressen		Anzahl	Hosts je Netz
A	10.0.0.0 - 10.255.255.255	1	2^{24}
B	172.16.0.0 - 172.31.255.255	16	2^{16}
C	192.168.0.0 - 192.168.255.255	256	2^8

Bei „Hosts je Netz“ die Netzwerk- und Broadcastadresse abziehen!



Nachteile der Klassendefinitionen

- **Ineffiziente Nutzung des Adressraums!**
 - Beispiel:
Ein Klasse-B-Netz belegt 65.536 Adressen, auch wenn in einer Organisation nur 2.000 tatsächlich genutzt werden
- **Folge war eine „künstliche“ Verringerung des verfügbaren Adressraumes**
- **Viele „alte“ Internet-Anwender hatten viel zu große Adressbereiche aus vor 1990**

CIDR

Classless InterDomain Routing



Netzwerk-Teil einer IP-Adresse kann von beliebiger Länge sein

■ Adressformat: a.b.c.d/x

wobei x die Anzahl der Bits im Netzwerk-Teil der Adresse darstellt

Netzwerk: 200.23.16.0/23

Netzwerk-Teil			Host-Teil
11001000	00010111	00010000	00000000

CIDR

Classless InterDomain Routing



Netzwerk-Teil einer IP-Adresse kann von beliebiger Länge sein

■ Adressformat: a.b.c.d/x

wobei x die Anzahl der Bits im Netzwerk-Teil der Adresse darstellt

Netzwerk: 200.23.16.0/23

Netzwerk-Teil			Host-Teil
11001000	00010111	00010000	00000000
11111111	11111111	11111110	00000000

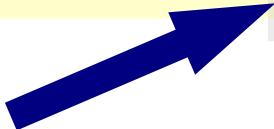
Netzmask: 255.255.254.0



Weitergabe von IP-Adressen

Ein ISP kann seinen zugewiesenen Bereich untergliedern, indem er den Netzwerk-Teil erweitert und damit Subnetze schafft!

ISP-Adressblock 11001000 00010111 00010000 00000000
200.23.16.0/20



Die Größe dieser Subnetze ist quasi beliebig, hängt von seinen Plänen ab!



Weitergabe von IP-Adressen

Ein ISP kann seinen zugewiesenen Bereich untergliedern, indem er den Netzwerk-Teil erweitert und damit Subnetze schafft!

ISP-Adressblock	<u>11001000 00010111 00010000</u>	00000000
	200.23.16.0/20	

Organisation A	<u>11001000 00010111 00010000</u>	00000000
	200.23.16.0/23	

Organisation B	<u>11001000 00010111 00010010</u>	00000000
	200.23.18.0/23	

Organisation C	<u>11001000 00010111 00010100</u>	00000000
	200.23.20.0/23	



Namen braucht die Welt!



Wer ist wer? Und wo?

Identifizierung von Menschen:

- Name + Geburtsdatum, Personalausweis, Sozialversicherungsnummer, ...

Aber Rechner oder Router?

- IP-Adresse (IPv4: 32 bit / IPv6: 128 bit) – benutzt von Rechnern zur Adressierung von Datagrammen – weltweit eindeutig
- Hostname – benutzt von Menschen (z.B. ftp.informatik.haw-hamburg.de) – ebenfalls weltweit eindeutig

Ein Teil der Antwort: Domain Name System (DNS)



- **Ein technischer Standard!**
- **Eine Sammlung von Protokollen!**
- **Eine verteilte Datenbank!**
- **Der kritischste Infrastrukturdienst für das Internet!**
- **Das System, das jeder von uns nutzt, wenn Emails geschrieben oder gesurft wird!**

Ein Teil der Antwort: Domain Name System (DNS)



DNS ist ein Protokoll der Anwendungsschicht, über das Endsysteme, Router und DNS-Server miteinander kommunizieren, um eine Abbildung von Hostnamen auf IP-Adressen – und umgekehrt – zu erreichen.

- DNS stellt einen Dienst für andere Anwendungsschicht-Protokolle zur Verfügung (ohne Benutzerschnittstelle), stellt also selbst keine Anwendung im engeren Sinne dar.
- DNS verwendet 53/udp, einige Verbindungen laufen aber auch über 53/tcp



Was ist DNS?

- Ein technischer Standard!
- Der kritischste Infrastrukturdienst für das Internet!
- Das System, das jeder von uns nutzt, wenn Emails geschrieben oder gesurft wird!



A(lice)



**Name Server
für bank.de**



Was ist DNS?

- Ein technischer Standard!
- Der kritischste Infrastrukturdienst für das Internet!
- Das System, das jeder von uns nutzt, wenn Emails geschrieben oder gesurft wird!





Was ist DNS?

- Ein technischer Standard!
- Der kritischste Infrastrukturdienst für das Internet!
- Das System, das jeder von uns nutzt, wenn Emails geschrieben oder gesurft wird!





Technische Bausteine des DNS

Zusammengesetzt aus vier Bausteinen:

■ Domain Names und Resource Records

Baumartige Strukturen für Hostnames und IPs

■ Name Servers

Informationen über eine Untermenge (Zones)

Authoritative, sofern vollständig und autorisiert

Primary und zugeordnete Secondary

Caching, sofern keine eigenen Informationen

■ Resolvers

stellen Anwendungen Informationen über Hostnames und IPs zur Verfügung

Name Server, /etc/hosts, NIS, LDAP, ...



Festgelegt in mehr als 250 RFCs!

Domain Name System (Ursprünge):

RFC1034 und 1035 (1987): Domain Names

RFC2181: Clarifications

RFC2308, 2671: Features

Sicherheitserweiterungen (Ursprünge):

RFC2535 (1999): DNSSEC, obsolete

RFC2845 (2000): TSIG

RFC2930 (2000): TKEY

RFC3007 (2000): Secure Dynamic Update



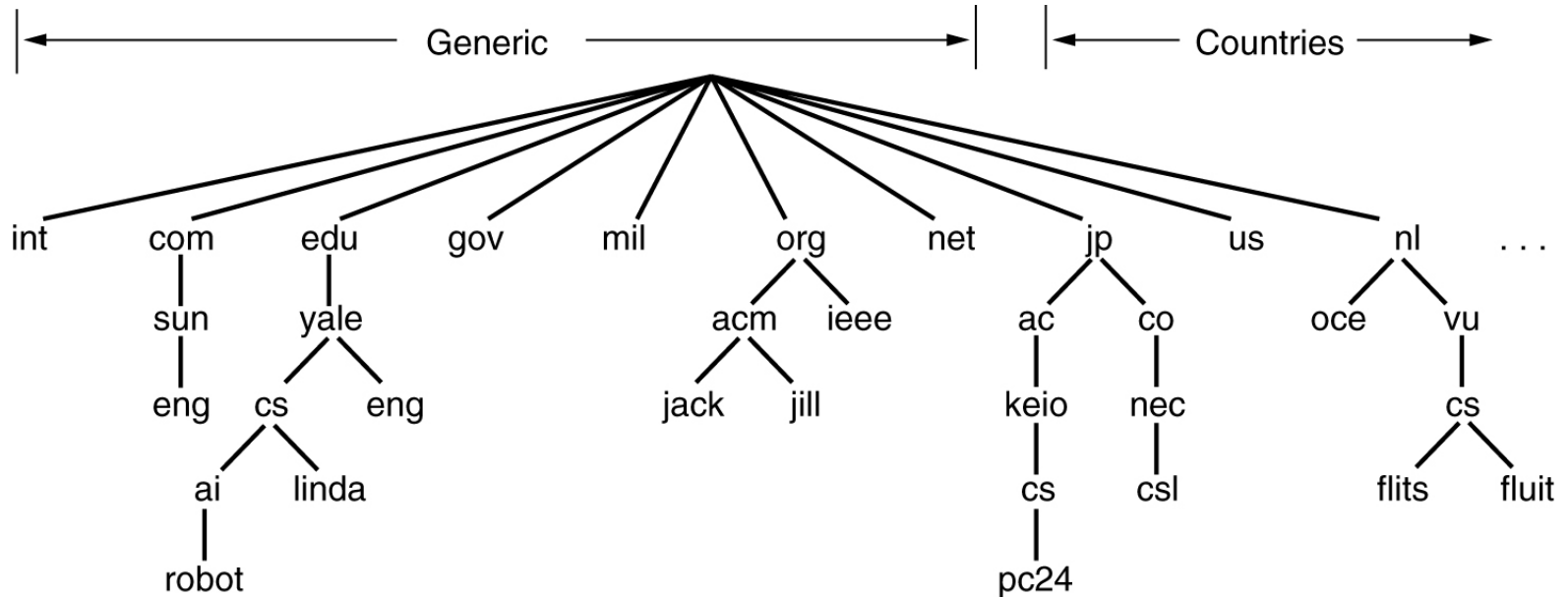
Das DNS-Konzept

Namen werden eingeführt, um die Adressierung im Internet für Menschen benutzbarer zu machen:

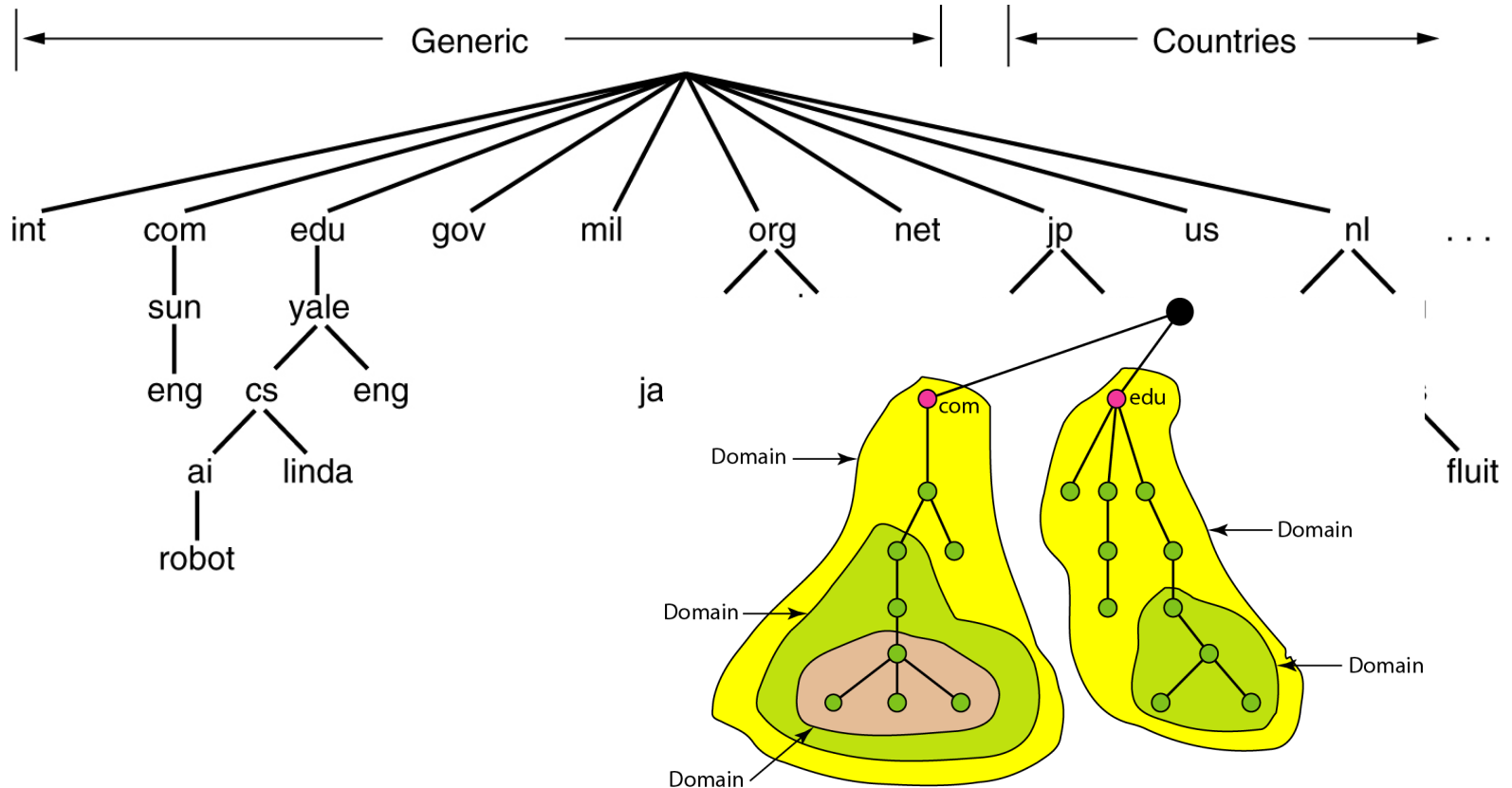
z.B. `www.haw-hamburg.de`

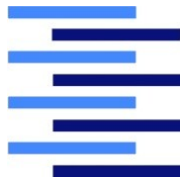
- **Namensraum ist hierarchisch und wird verteilt gepflegt bzw. verantwortet**
- **Von der Wurzel („.“) ausgehende global Top-Level Domains (gTLD)**
 - über die NICs organisiert

Die DNS-Hierarchie



Die DNS-Hierarchie





DNS Resource Records

- Einträge in der verteilten Datenbank heißen Resource Records (RR)
 - Für einen Host sind beliebig viele Einträge möglich
- Ein Resource Record besteht aus den Werten
 - Domain_name
 - Time_to_live
 - Class
 - Type
 - Value

Beispiel:

www.is.haw-hamburg.de	172800	IN	A	141.22.192.150
-----------------------	--------	----	---	----------------



DNS Resource Record (RR)

Typ	Bedeutung	Wert
SOA	Start of Authority	Parameter für diese Zone (mehrere Attribute)
A	Adresse eines Hosts (IPv4)	32-Bit integer
AAAA	Adresse eines Hosts (IPv6)	128-Bit integer
MX	Mail eXchange	16-Bit integer (Prioritätsangabe), danach Name eines Mailservers
NS	Name Server	Name-Server-Adresse für eine Domain



DNS Resource Record (RR)

Typ	Bedeutung	Wert
CNAME	Canonical name	Domainname
PTR	Pointer	Name für eine IP-Adresse ("Reverse Lookup")
HINFO	Host description	CPU und BS in ASCII
TXT	Text	Uninterpretierter ASCII-Text

DNS Resource Record (RR)

Beispiel (sehr alt)



; Authoritative data for cs.vu.nl

cs.vu.nl.	86400	IN	SOA	star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.	86400	IN	TXT	"Divisie Wiskunde en Informatica."
cs.vu.nl.	86400	IN	TXT	"Vrije Universiteit Amsterdam."
cs.vu.nl.	86400	IN	MX	1 zephyr.cs.vu.nl.
cs.vu.nl.	86400	IN	MX	2 top.cs.vu.nl.

flits.cs.vu.nl.	86400	IN	HINFO	Sun Unix
flits.cs.vu.nl.	86400	IN	A	130.37.16.112
flits.cs.vu.nl.	86400	IN	A	192.31.231.165
flits.cs.vu.nl.	86400	IN	MX	1 flits.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	2 zephyr.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	3 top.cs.vu.nl.
www.cs.vu.nl.	86400	IN	CNAME	star.cs.vu.nl
ftp.cs.vu.nl.	86400	IN	CNAME	zephyr.cs.vu.nl

DNS Resource Record (RR)

Beispiel (sehr neu)



```
> host -l cs.vu.nl.  
; Transfer failed.  
Host cs.vu.nl not found: 5(REFUSED)  
; Transfer failed.
```



DNS-Format der Nachrichten

Es gibt Anfrage- und Antwortnachrichten, beide haben dasselbe Nachrichtenformat!

- **identification:**

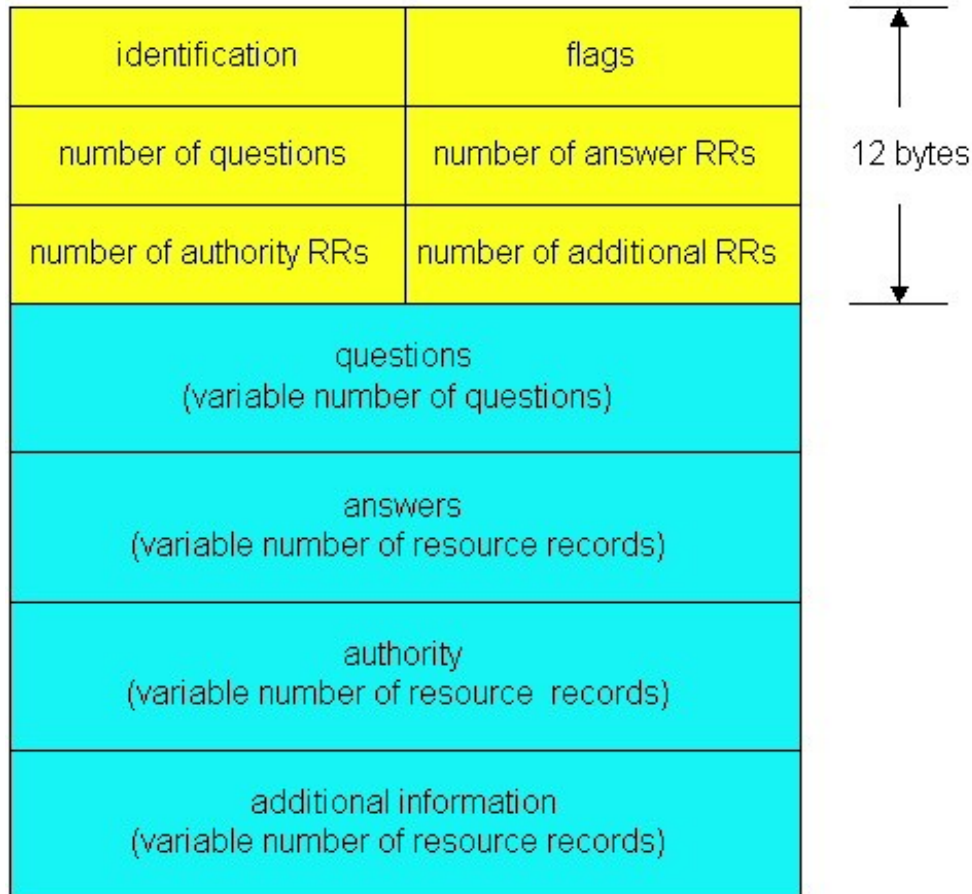
- 16 bit-Zahl zur Identifizierung einer Anfrage und zugehörigen Antwort

- **Flags:**

- Anfrage oder Antwort?
- Rekursion gewünscht?
- Rekursion verfügbar?
- Antwort ist autoritativ!



DNS-Format Nachrichten



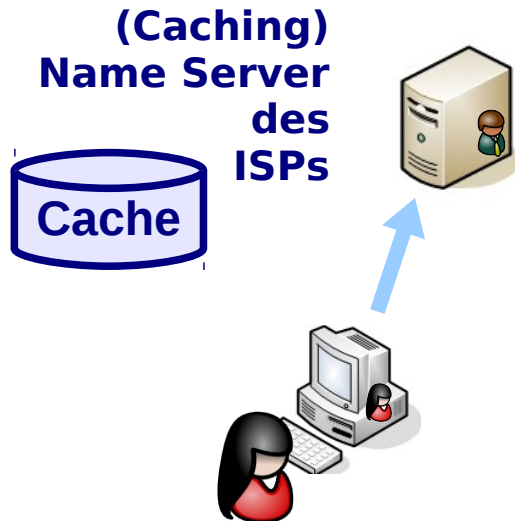
Ablauf der DNS-Auflösung



**www.
bank.
de**

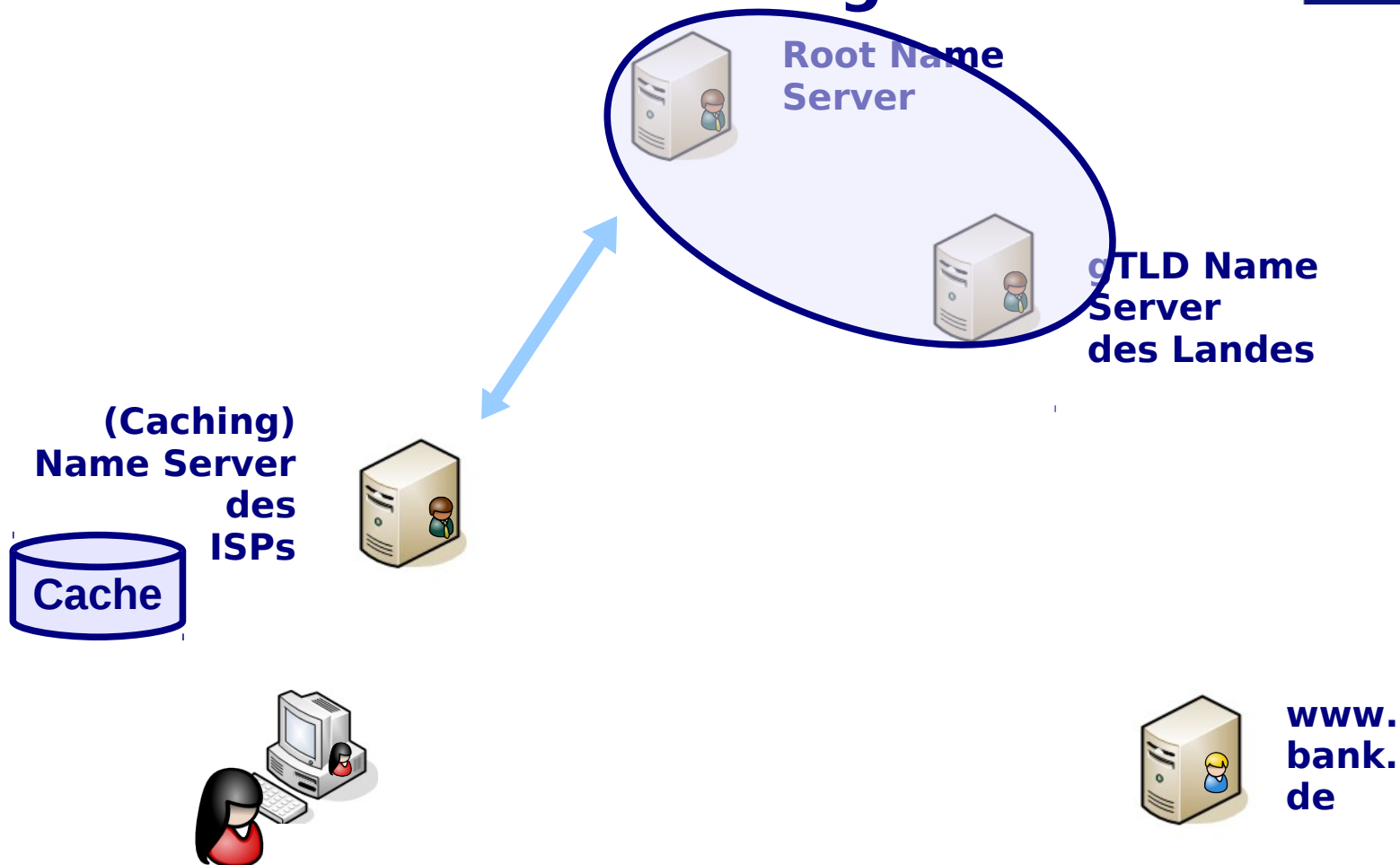


Ablauf der DNS-Auflösung

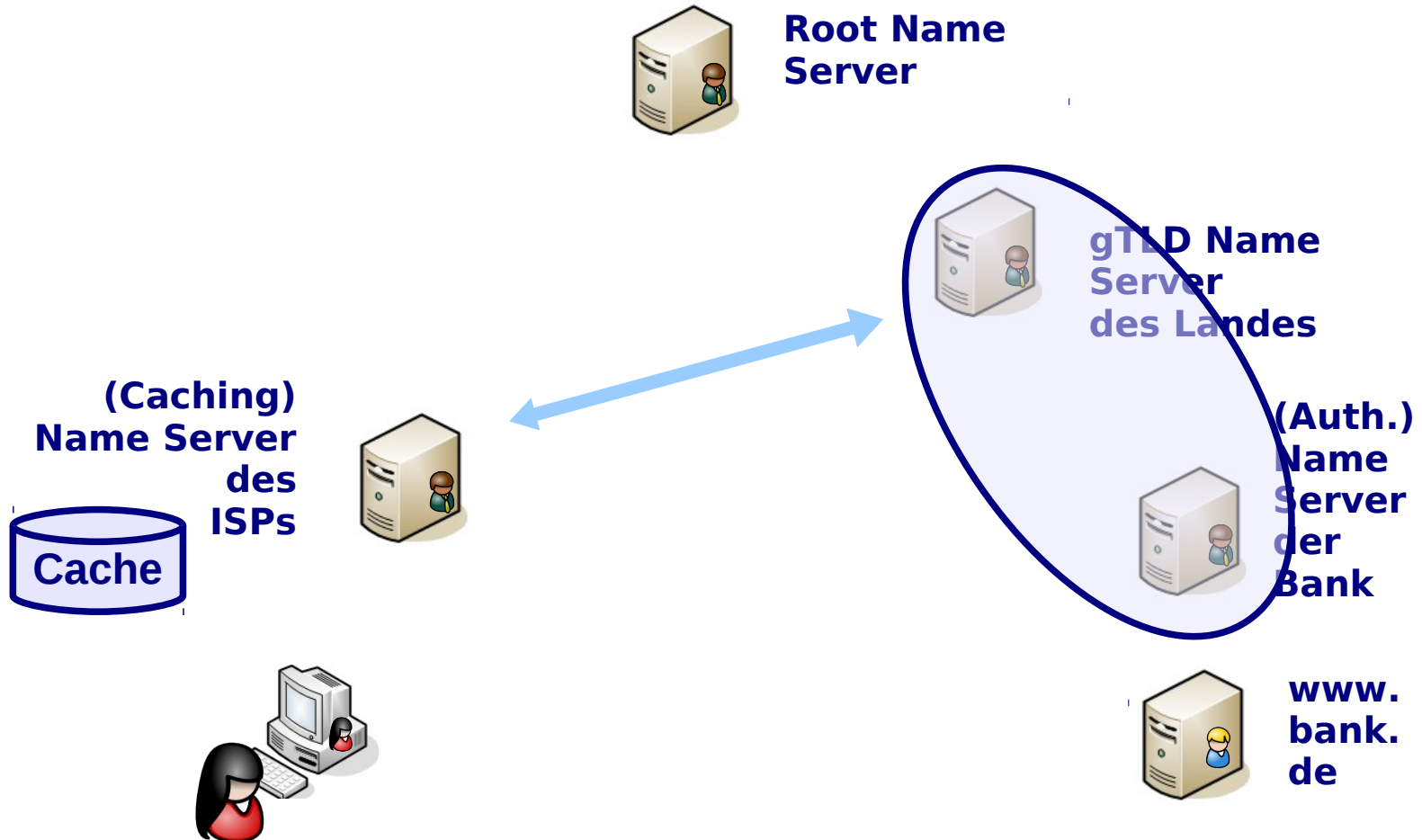




Ablauf der DNS-Auflösung



Ablauf der DNS-Auflösung



Ablauf der DNS-Auflösung

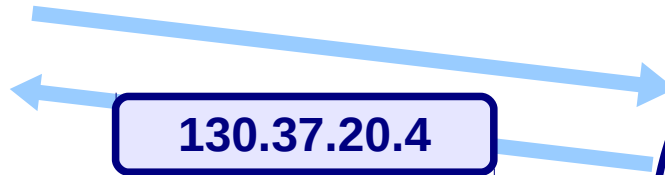


**Root Name
Server**



**gTLD Name
Server
des Landes**

**(Caching)
Name Server
des
ISPs**



130.37.20.4

**(Auth.)
Name
Server
der
Bank**



**www.
bank.
de**

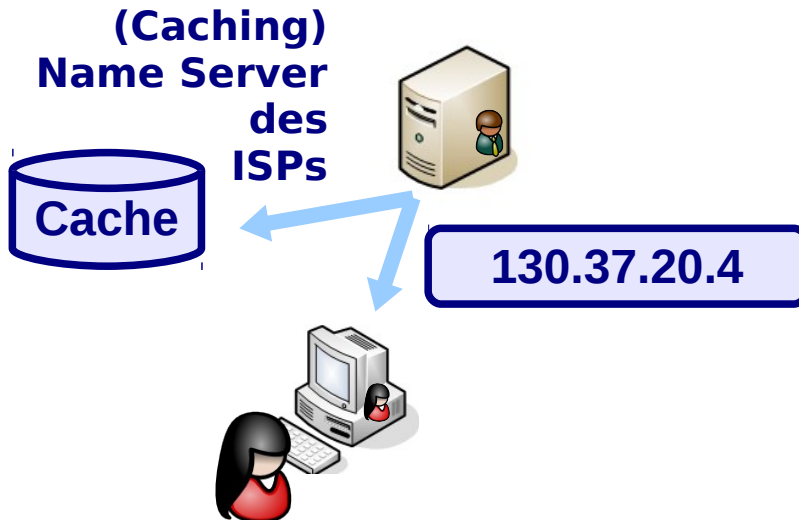
Ablauf der DNS-Auflösung



**Root Name
Server**



**gTLD Name
Server
des Landes**



Verwaltung durch verteilte DNS - “Name - Server”



Warum gibt es keinen zentralen Name-Server für das gesamte Internet?

- **Single point of failure**
- **Verkehrslast**
- **Entfernung der zentralen Datenbank**
- **Wartung**

Diese Architektur wäre nicht skalierungsfähig!



Arten von Name-Servern

■ Lokale Name-Server:

- jeder ISP / jede Firma hat üblicherweise einen lokalen Name-Server ("DNS-Server")
- Alle DNS-Anfragen eines Hosts gehen zuerst zum lokalen Name-Server (IP-Adresse des lokalen DNS-Servers gehört zur IP-Konfiguration eines Hosts)
- Lokale Nameserver erfragen IP-Adressen bei autoritativen Nameservern



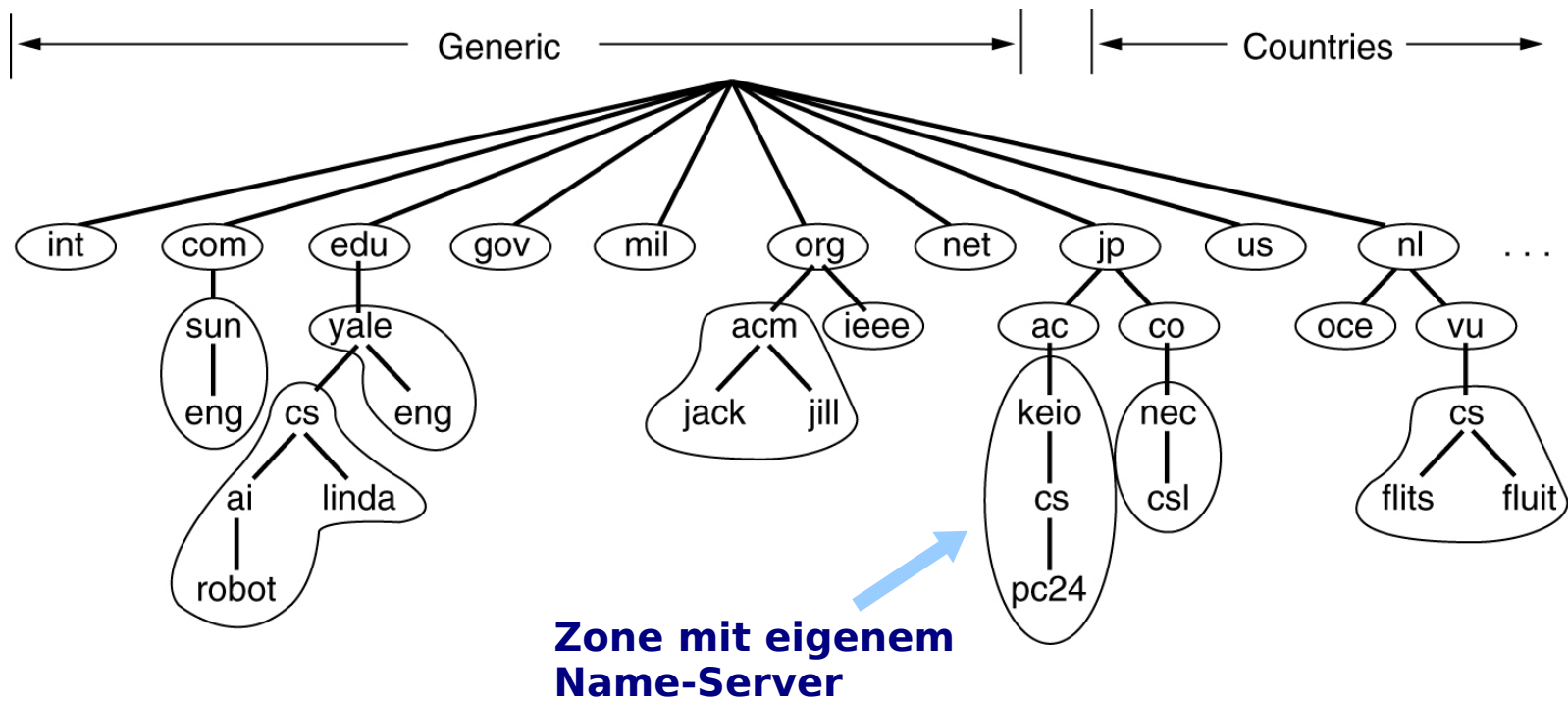
Arten von Name-Servern (2)

■ Autoritative Name-Server:

- sind verantwortlich für die Speicherung von Name und IP-Adresse von Hosts
- können Anfragen zur Umrechnung von Namen in IP-Adressen beantworten (und noch mehr ...)
- verwalten eine “Zone” des Namensraums als “Autorität”



Authoritative Name-Server

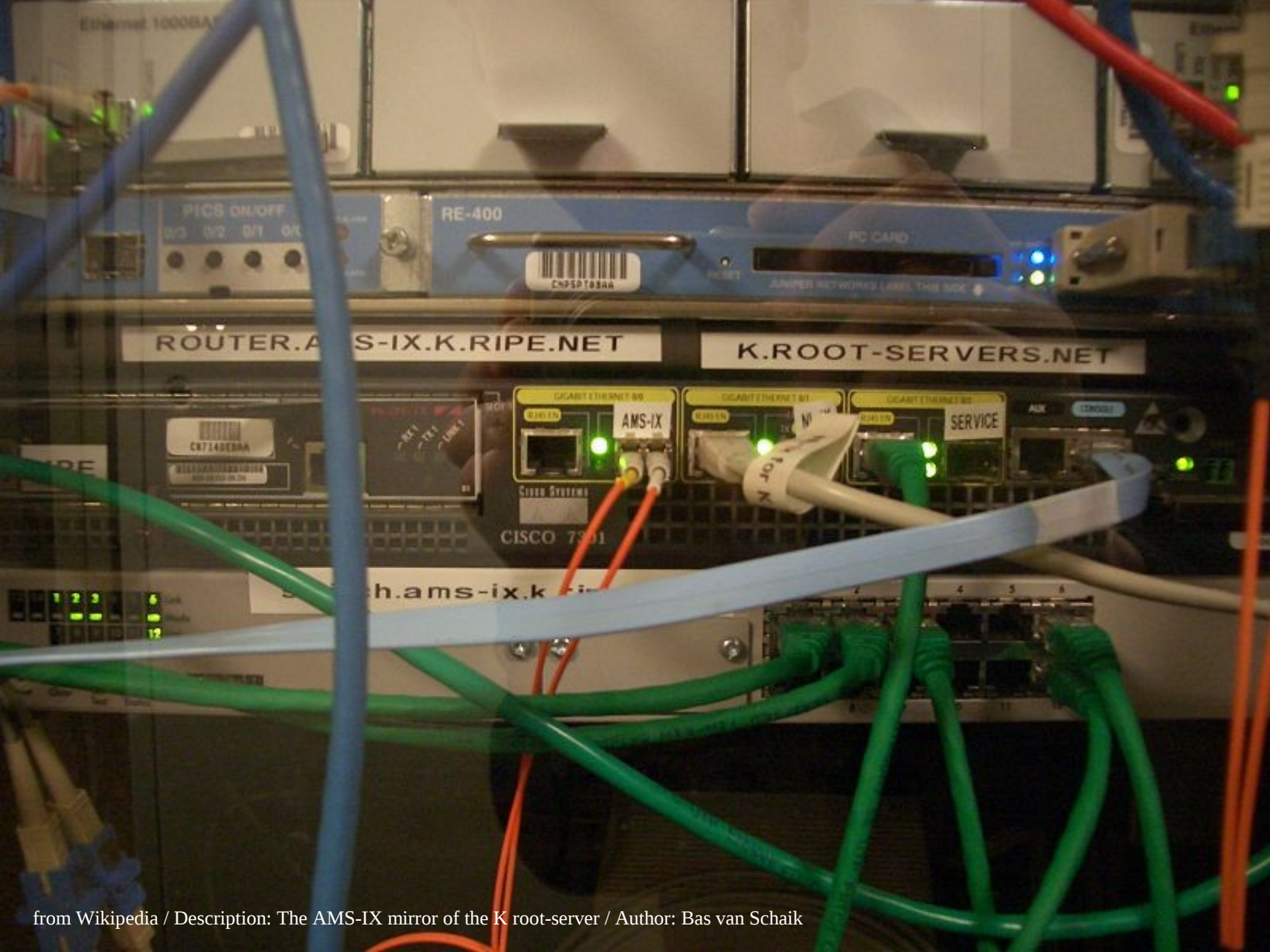




Arten von Name-Servern (3)

■ Root-Name-Server

- verweisen auf autoritative Name-Server für die Top-Level Domains (com, org, edu, de, nl, uk, jp, ...)
- lokale Name-Server kontaktieren diese, wann immer Hostname nicht aufgelöst werden kann
- die Adressen der Top-Level-Domain-Nameserver sind jedoch meist im Cache der lokalen Name-Server vorhanden

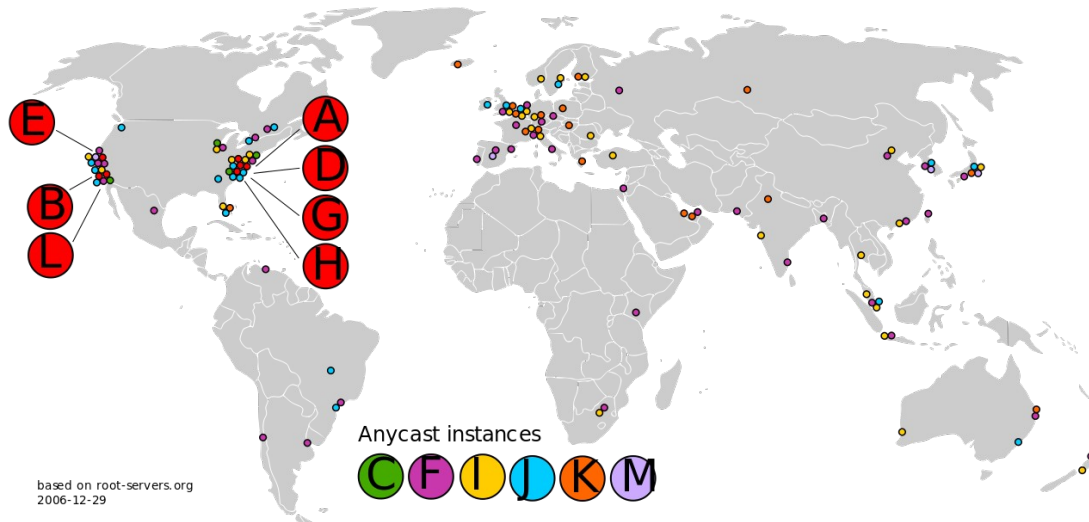


from Wikipedia / Description: The AMS-IX mirror of the K root-server / Author: Bas van Schaik



Root Name-Server

- liefern den im Pfad nächsten autoritativen Name-Server zum angefragten Hostname



Weltweit gibt es 13 Root Name-Server-Einträge.

Durch ANYCAST tatsächlich mehrere 100 Rechner.

IP-Adressen der Root-Name-Server sind durch eine Konfigurations-datei allen anderen Name-Servern bekannt!



Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell
- Netzwerk als Infrastruktur
 - Adressierung, DNS und andere Details
 - Entwicklung im Internet
- Layer 7: Anwendungsschicht
- Layer 7/4: Socketprogrammierung
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
- Layer 2: Sicherungsschicht



Organisation im Internet

- Die Internet Society (ISOC) vertritt seit 1992 die Belange des Internets nach außen
- Die Internet Corporation for Assigned Names and Numbers (ICANN) administriert den Namensraum und entwickelt ihn weiter



Vergabe von IP-Adressen

■ ICANN

- vergibt IP-Adressbereichen an ISPs sowie große Organisationen
- verwaltet DNS-Top-Level-Domains und
- betreibt die DNS-Root-Server
- delegiert technische Durchführung

■ IANA

- Delegiert die regionale Koordinierung (RIR) an
 - APNIC (Asia Pacific Network Information Centre)
 - ARIN (American Registry for Internet Numbers)
 - LACNIC (Regional Latin-American and Caribbean IP Address Registry)
 - RIPE NCC (Réseaux IP Européens)



Vergabe von IP-Adressen (2)

- **Regional Internet Registries (RIR)** zusammenhängende Adressbereiche an ISPs
- **ISPs vergeben zusammenhängende Adressbereiche an ihre Kunden**
- **Dadurch wird erst die Aggregation in Routing-Tabellen möglich, die durch das sogenannte Classless Interdomain Routing (CIDR) verwendet wird**



Organisation im Internet (2)

- Die Internet Society (ISOC) vertritt seit 1992 die Belange des Internets nach außen
- Die Internet Corporation for Assigned Names and Numbers (ICANN) administriert den Namensraum und entwickelt ihn weiter
- Die Internet Assigned Number Authority (IANA) weist Protokollparameter zu und betreibt Namens- und Adressservices
- IAB, IESG, IETF und IRTF kümmern sich um die technischen Standards



Organisation im Internet (3)

- **Die Koordinierung und (technische) Weiterentwicklung wird vom Internet Architecture Board (IAB) geleitet mit:**
 - Internet Research Task Force (IRTF)
für langfristige Forschungsaufgaben
 - Internet Engineering Task Force (IETF)
für die technische Weiterentwicklung
 - Internet Engineering Steering Group (IESG)
- **Die Verbreitung von Standards geschieht auf der Grundlage von technischen Reports, den Requests for Comments**



Besondere Spielregeln bei IETF

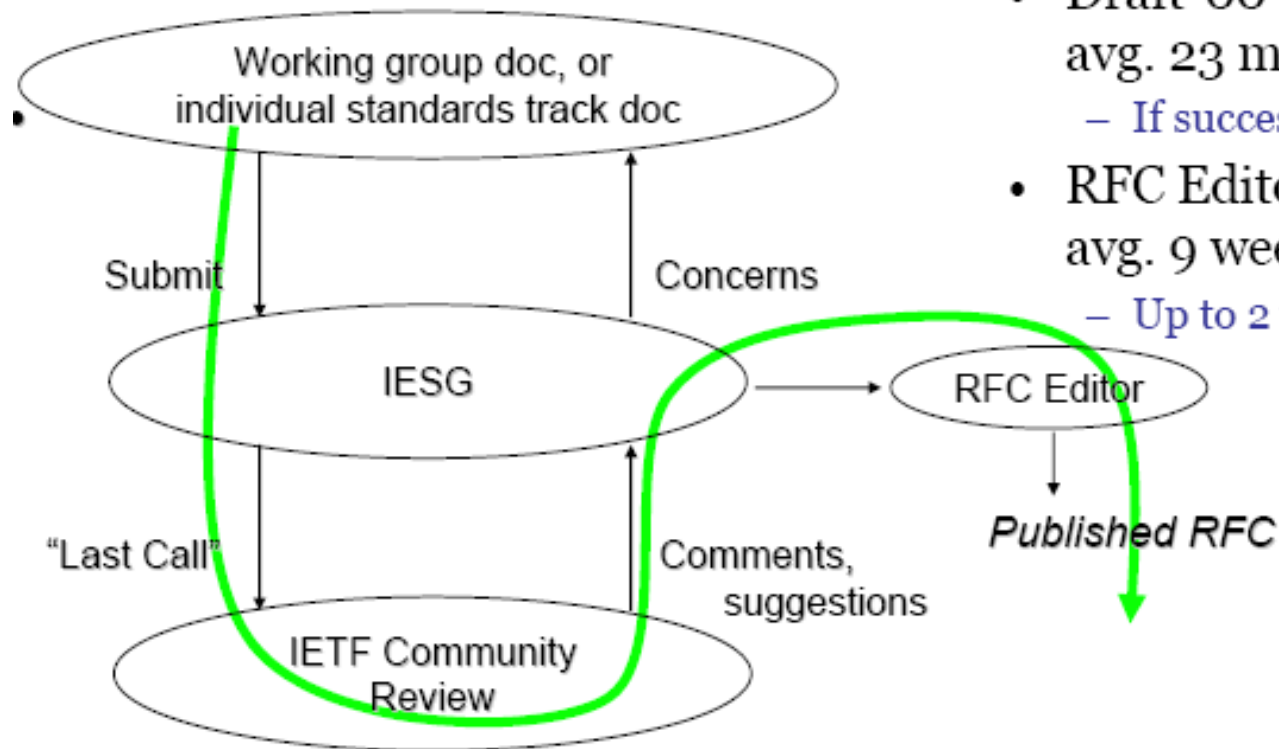
- does not exist (in a legal sense), **no** members, **no** voting
 - Groups make decisions by “**rough consensus & running code**”
 - “*We reject kings, presidents and voting. We believe in rough consensus and running code*”, David Clark, 1992
 - Consensus must be found on mailing lists rather than at physical meetings
- 118ish **working groups** (where the stuff happens)
- 8 **areas** (for organizational convenience) with **ADs**
 - GEN, APS, **RAI**, TSV, RTG, INT, OPS, SEC
- **IESG**: management (ADs + IETF Chair)
- produces **standards** and other



Request for Comments (RFCs)

- Zur Erarbeitung eines Internet-Standards kann jeder Mensch einen technischen Report, die sog. Internet Drafts einsenden
- Nach Publikation und Diskussion in Working Groups werden diese ggf. zu RFCs
- RFCs für Protokolle durchlaufen die Stati:
 - proposed
 - implementation
 - draft
 - full standard

Der IETF-Standardisierungsprozess



- Draft-00 → RFC:
avg. 23 months
– If successful
- RFC Editor Queue:
avg. 9 weeks
– Up to 2 years



Kontakt

Prof. Dr. Klaus-Peter Kossakowski

**Email: klaus-peter.kossakowski
@haw-hamburg.de**

Mobil: +49 171 5767010

<http://users.informatik.haw-hamburg.de/~kpk/>