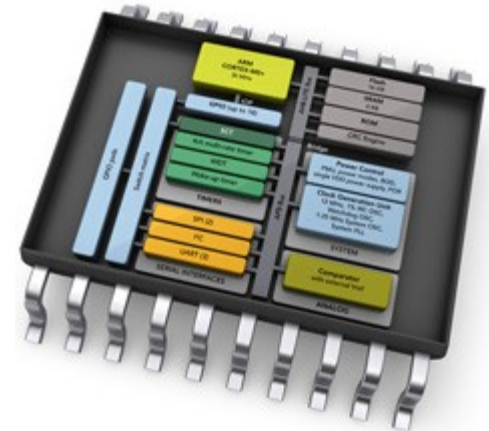


Kommunikationssysteme

(Modulcode 941306)

Prof. Dr. Andreas Terstegge

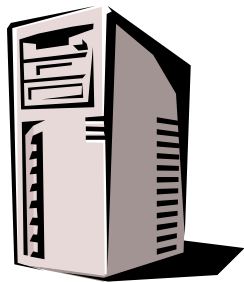


Domain Name System

Lesbare Adressen im Internet

Semantische/mnemonicische Namen (DNS)

- Socket-basierte Kommunikation nutzt IP-Adressen
- End-Anwender wollen sprechende Bezeichnungen
mnemonisch
Eigenschaften von Bezeichnungen und Namen, wenn sie leicht zu merken sind und Rückschlüsse auf ihre Bedeutung haben.
- End-Anwender wollen stabile Namen für einen Service, und keine neue IP nach einem Umzug des Servers
- **DNS** = Domain Name System
→ Namen müssen übersetzt und aufgelöst werden

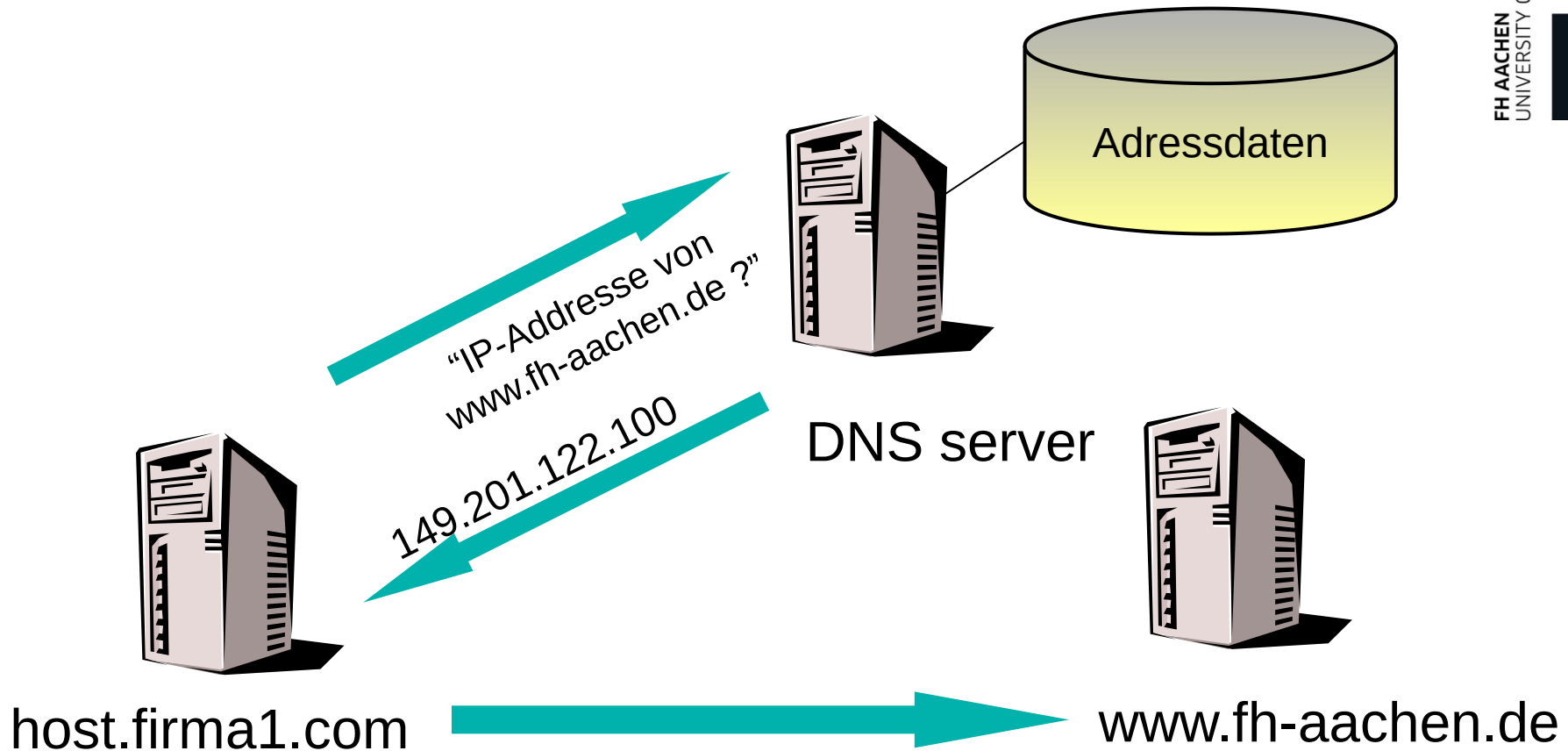


host.firma1.com

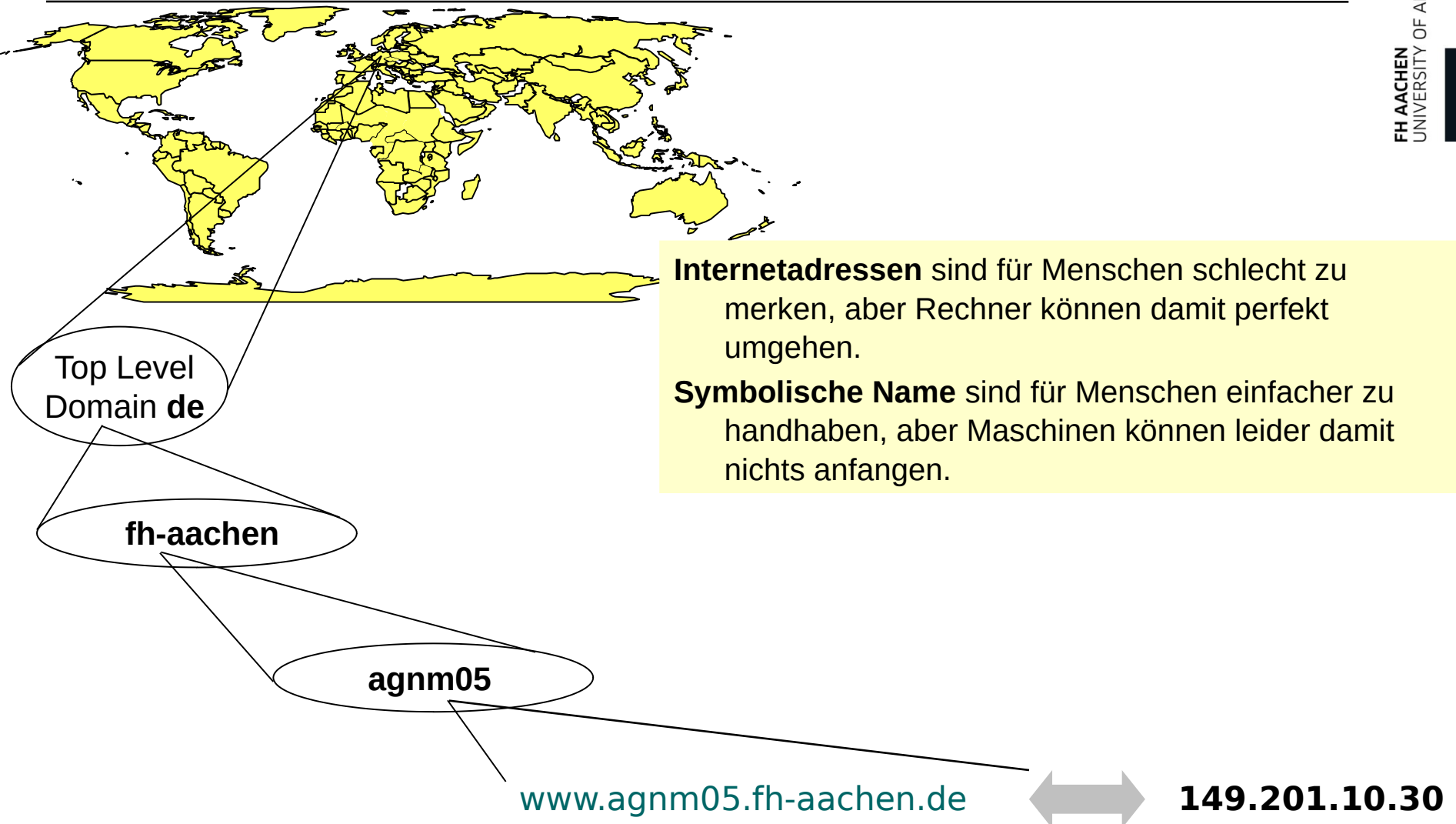


www.fh-aachen.de

Im Programmcode verankerter “Lookup”

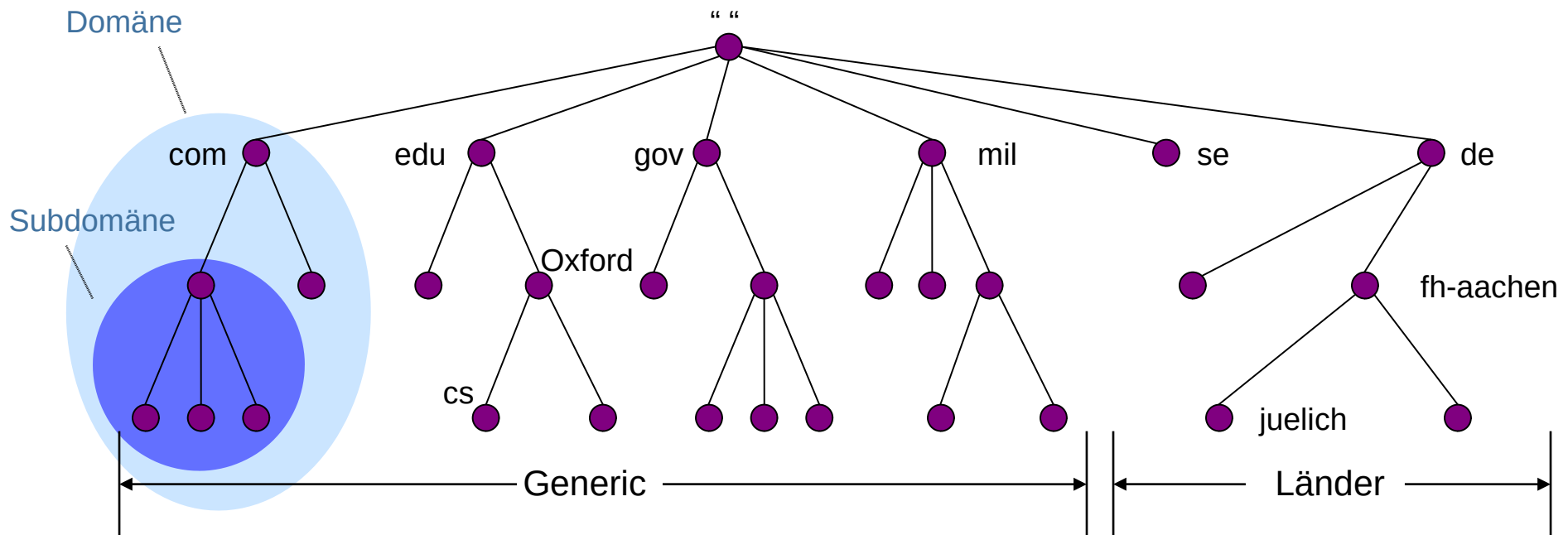


DNS - Domain Name System



Struktur der Datenbank

- Zur Strukturierung aller Informationen: Datenbank lässt sich als **Baum** darstellen
- jeder Knoten des Baums ist mit einem Label beschriftet, das ihn relativ zum Vaterknoten identifiziert
- jeder (innere) Knoten ist wiederum selber Wurzel eines Teilbaums
- jeder dieser Teilbäume repräsentiert eine **Domäne**
- jede Domäne kann wiederum weiter in **Subdomänen** unterteilt werden



Struktur der Datenbank:

Generische Top level Domains

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes

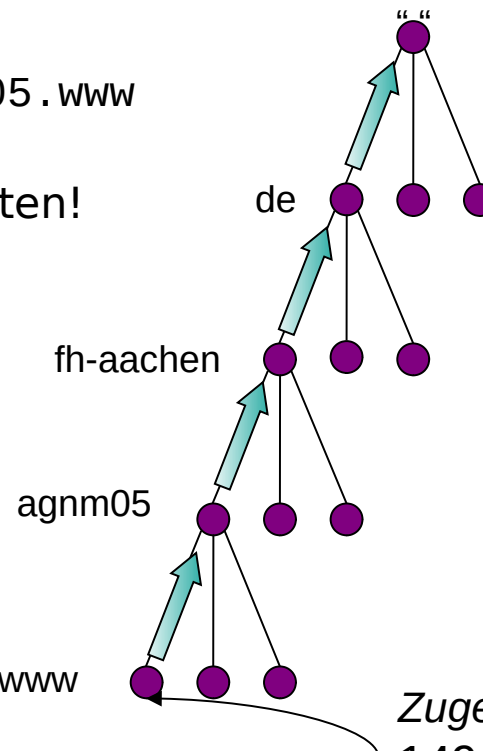
Domännennamen

- der Name einer Domäne besteht aus der Folge von Labeln (getrennt durch „.“) beginnend beim ‚Blatt‘ der Domäne und aufsteigend bis zur Wurzel des Gesamtbaums
- In den Blattknoten sind die IP-Adressen der durch die Labelsequenz gegebenen Namen gespeichert
- Eine Darstellung `de.fh-aachen.agnm05.www` wäre logischer, aber weniger lesbar
- Daher: Auflösung des Namens von hinten!

logischer Name:

www.agnm05.fh-aachen.de

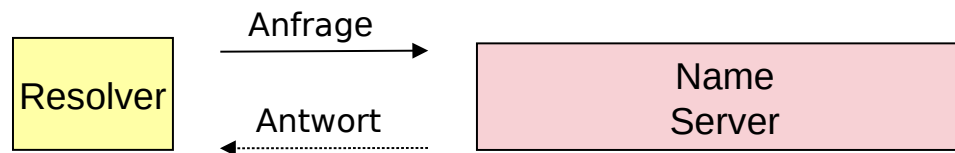
www



Zugehörige IP-Adresse:
149.201.10.30

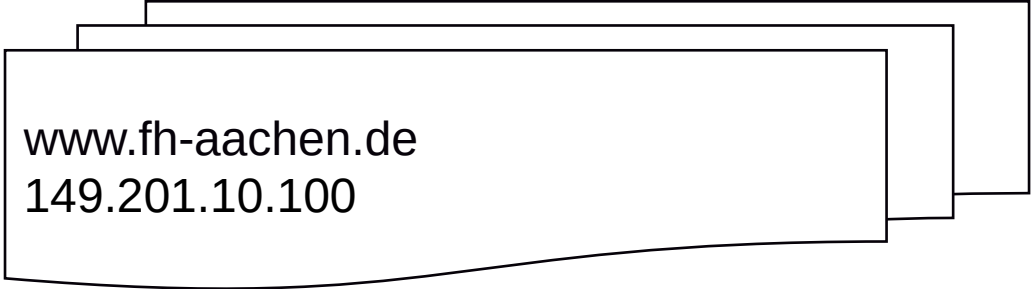
DNS - Konzept

1. DNS handhabt die Abbildung von Rechnernamen auf Adressen (**und weitere Dienste**)
2. DNS ist eine **verteilte Datenbank**, d.h. die einzelnen Segmente unterliegen einer *lokalen Kontrolle*
3. Die Struktur des verwendeten **Namensraums** der Datenbank **gibt die administrative Einteilung des Internets wider**
4. Daten jedes lokalen Bereichs sind mittels einer Client/Server-Architektur im gesamten Netzwerk verfügbar
5. Robustheit und Geschwindigkeit des Systems werden durch Replikation der Daten und Zwischenspeicherung (engl. *Caching*) erreicht
6. Hauptkomponenten:
 - **Name Server:** Server, die Informationen über einen Bereich der Datenbank verwalten
 - **Resolver:** Clients, die Anfragen an die Server stellen



DNS-Server

- Server-Prozess im Netz (z.B. im DSL-Router)
- Wartet auf Anfragen (UDP!)
- Enthält eine **Tabelle** mit **Namen** von lokalen Hosts und zugehörigen **IP-Adressen** (nicht injektiv)
- Wird von den Klienten über Konfigurationsdatei oder DHCP gefunden
- Zusammenspiel mit lokaler Datei auf Resolver-Seite
 /etc/hosts (UNIX) c:\WINDOWS\system32\drivers\etc (Windows)
- Reihenfolge bei manchen Systemen einstellbar:
 /etc/resolv.conf /etc/nsswitch.conf (UNIX)



www.fh-aachen.de
149.201.10.100

Zugriff auf entfernte Rechner

URL

http://www.agnm05.fh-aachen.de:80/index.html

DNS Lookup

IP-Adresse, Portnummer, Pfad

149.201.10.30

80

Index.html

ARP Lookup im Zielnetz

Hardware-Adresse

2:60:8c:2:b0:5a

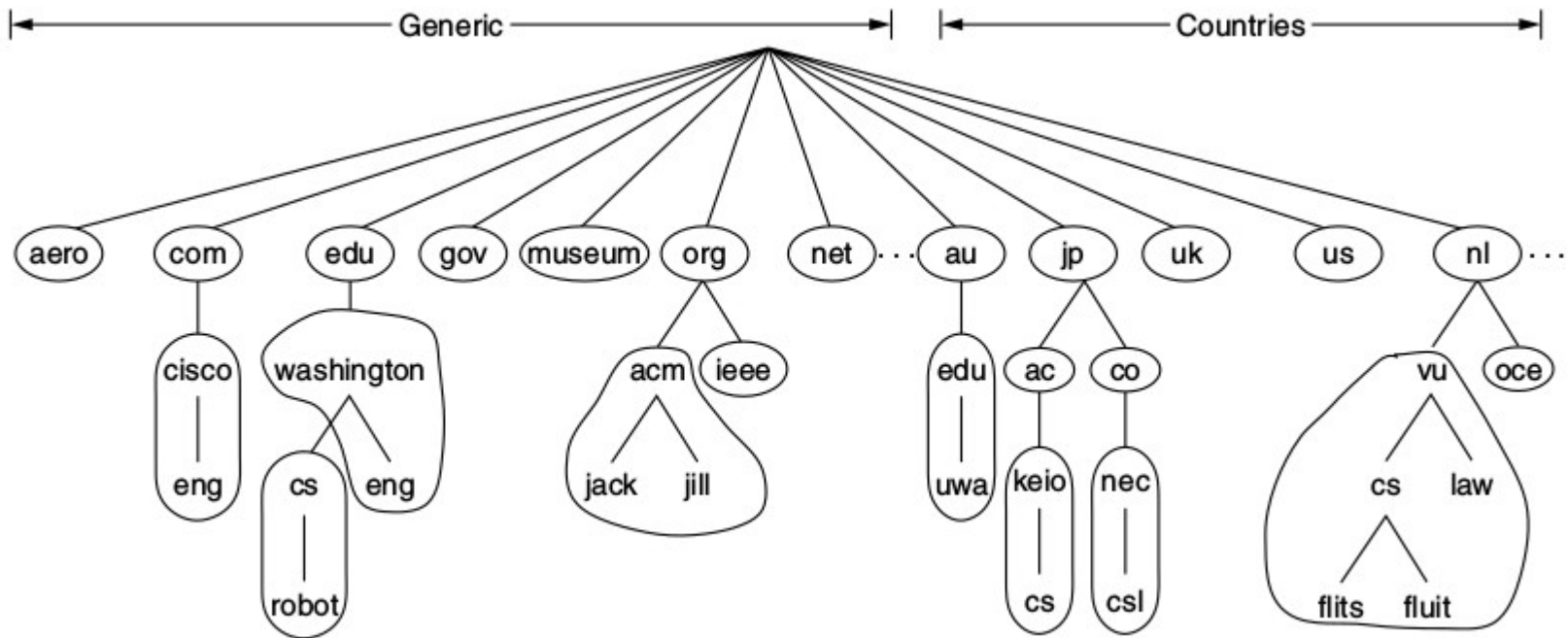
Socket

Web-Server

index.html

Domänen und Zonen

- Jeder Name Server verwaltet eine **Zone**, das ist ein Teil des Domänenbaumes
- Domäne und Zone sind unterschiedliche Konzepte:



- **Zonen** sind (außer in den ‚tieferen‘ Bereichen des Baumes) meistens nur für ein Namens-element einer Domänen zuständig (dann müssen vom Name Server weniger Informationen verwaltet werden)










- Eine Zone ist ein autarker und gemeinsam administrierter Bereich im DNS-Namensraum
- Jede Zone hat einen **primären** und beliebig viele **sekundäre Nameserver (NS)**
 - Jeder NS kennt nur einen Ausschnitt des gesamten Namensraums
 - Jeder NS kennt **alle IP-Adressen** seiner **direkt** untergeordneten Sub-Domains
 - Sekundäre NS führen ein periodisches Update („Zonentransfer“) ihrer Datenbasis durch (vollständige Datenbestand des primären NS wird transferiert) (Master-Slave-Prinzip)
- Zur Einrichtung einer Zone muss der übergeordnete Knoten davon überzeugt werden, die Verwaltung zu delegieren
- Eine Zone ist ein Namensraum mit eigener Datenbank
 - Knoten im Baum (Bezeichnung darf maximal 63 Zeichen lang sein)
 - Bis zu 127 Ebenen (ohne Bezeichnung)

DNS: Root-Name-Server

- Bilden die Wurzel der hierarchischen DNS-Struktur
- Es gibt weltweit 13 Root-Name-Server
 - z.Zt. {a-m}.root-servers.net
 - Die tatsächliche Anzahl der Server ist deutlich größer, da mit IPv6 hier Anycast-Adressen greifen können, so dass mehrere physikalische Server einen DNS-Root-Server realisieren können. Stichwort Anycast !
- Root-Server müssen hohe Anforderungen an die bearbeitbaren Lasten erfüllen
- Name-Server der tieferen Hierarchien werden mit festen Root-Servern konfiguriert (über bekannte IP-Adressen, meistens IPv6).

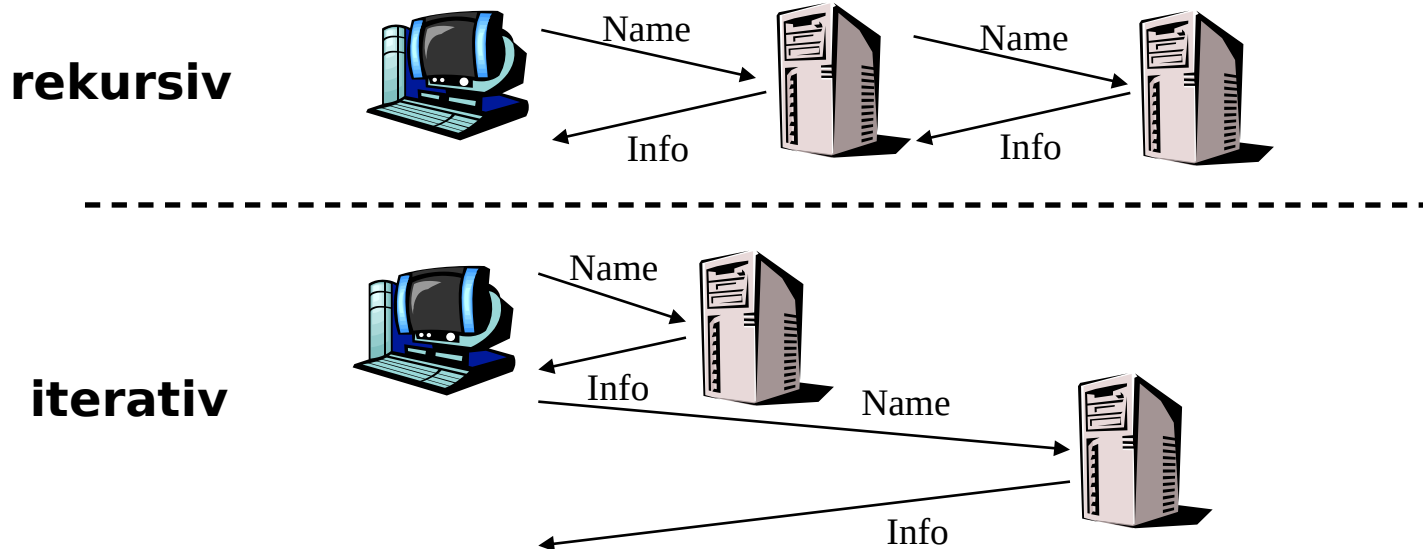
DNS: Root-Name-Server

Bekannte IPs

Letter ⇅	IPv4 address ⇅	IPv6 address ⇅	AS-number ^[9] ⇅	Old name ⇅	Operator ⇅
A 	198.41.0.4	2001:503:ba3e::2:30	AS19836, ^{[9][note 1]} AS36619, AS36620, AS36622, AS36625, AS36631, AS64820 ^{[note 2][11]}	ns.internic.net	Verisign
B 	199.9.14.201 ^{[note 3][12][13]}	2001:500:200::b ^[14]	AS394353 ^[15]	ns1.isi.edu	USC-ISI
C 	192.33.4.12	2001:500:2::c	AS2149 ^{[9][17]}	c.psi.net	Cogent Communications
D 	199.7.91.13 ^{[note 4][18]}	2001:500:2d::d	AS27 ^{[9][19]}	terp.umd.edu	University of Maryland
E 	192.203.230.10	2001:500:a8::e	AS21556 ^{[9][21]}	ns.nasa.gov	NASA Ames Research Center
F 	192.5.5.241	2001:500:2f::f	AS3557 ^{[9][22]}	ns.isc.org	Internet Systems Consortium
G  ^[note 5]	192.112.36.4 ^[note 6]	2001:500:12::d0d ^[note 6]	AS5927 ^{[9][24]}	ns.nlc.ddn.mil	Defense Information Systems Agency
H 	198.97.190.53 ^{[note 7][25]}	2001:500:1::53 ^{[note 8][25]}	AS1508 ^{[25][note 9][26]}	aos.arl.army.mil	U.S. Army Research Lab
I 	192.36.148.17	2001:7fe::53	AS29216 ^{[9][27]}	nic.nordu.net	Netnod

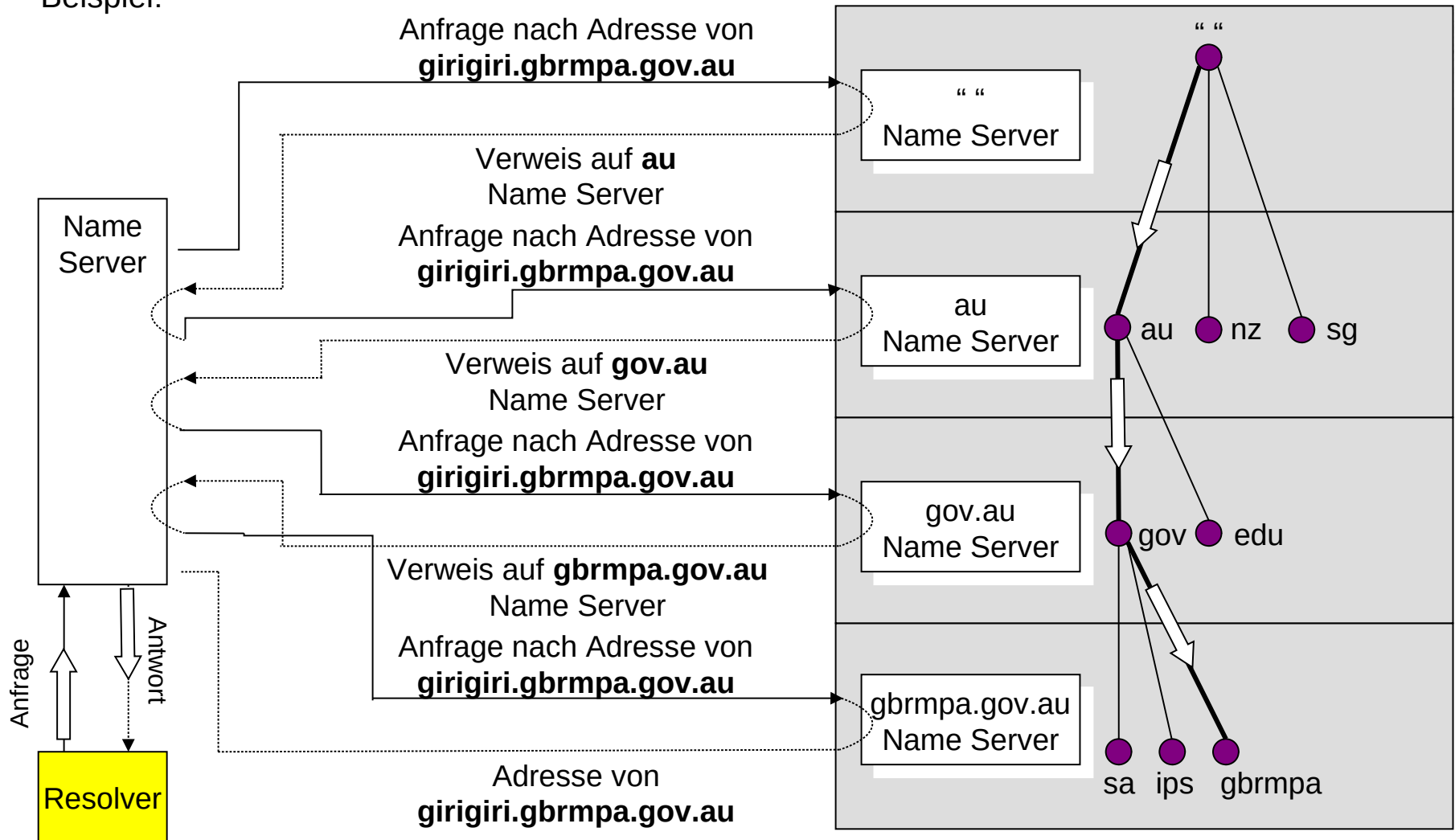
Die Auflösung: Rekursive und Iterative Anfragen

- Rekursive Anfragen -
Server schickt Anfrage zum nächsten Server weiter (oder Fehlermeldung). → Client-Server-Anfragen
- Iterative Anfragen -
Server antwortet dem Fragenden direkt mit IP-Adresse des nächsten Servers. → Server-Server-Anfragen



Namensauflösung: Iterativ

Beispiel:



- DNS leistet mehr als nur die Auflösung von Namen
- Der **Mail-Exchange-Record** liefert zu einer Zone den Mail-Server (so erhält man das wissen, wer bei der FH-Aachen die Mails empfängt)
- Weitere Informationen können z.B. im Zusammenhang mit der IP-Telefonie geliefert werden
- Jeder DNS-Server besitzt auch einen **Cache**. Dieser hält vor kurzem aufgelöste Anfragen vor. Den Zeitraum liefert der Server, der diese Adresse ursprünglich einmal aufgelöst hat

DNS-Datenbank: : Domain Resource Records

; Authoritative data for cs.vu.nl

cs.vu.nl.	86400	IN	SOA	star boss (9527,7200,7200,241920,86400)
cs.vu.nl.	86400	IN	MX	1 zephyr
cs.vu.nl.	86400	IN	MX	2 top
cs.vu.nl.	86400	IN	NS	star

Beispiel: Einträge des
Nameservers für cs.vu.nl

$24 \cdot 60 \cdot 60s = 86400s$

star	86400	IN	A	130.37.56.205
zephyr	86400	IN	A	130.37.20.10
top	86400	IN	A	130.37.20.11
www	86400	IN	CNAME	star.cs.vu.nl
ftp	86400	IN	CNAME	zephyr.cs.vu.nl

flits	86400	IN	A	130.37.16.112
flits	86400	IN	A	192.31.231.165
flits	86400	IN	MX	1 flits
flits	86400	IN	MX	2 zephyr
flits	86400	IN	MX	3 top

rowboat		IN	A	130.37.56.201
		IN	MX	1 rowboat
		IN	MX	2 zephyr

little-sister		IN	A	130.37.62.23
---------------	--	----	---	--------------

laserjet		IN	A	192.31.231.216
----------	--	----	---	----------------

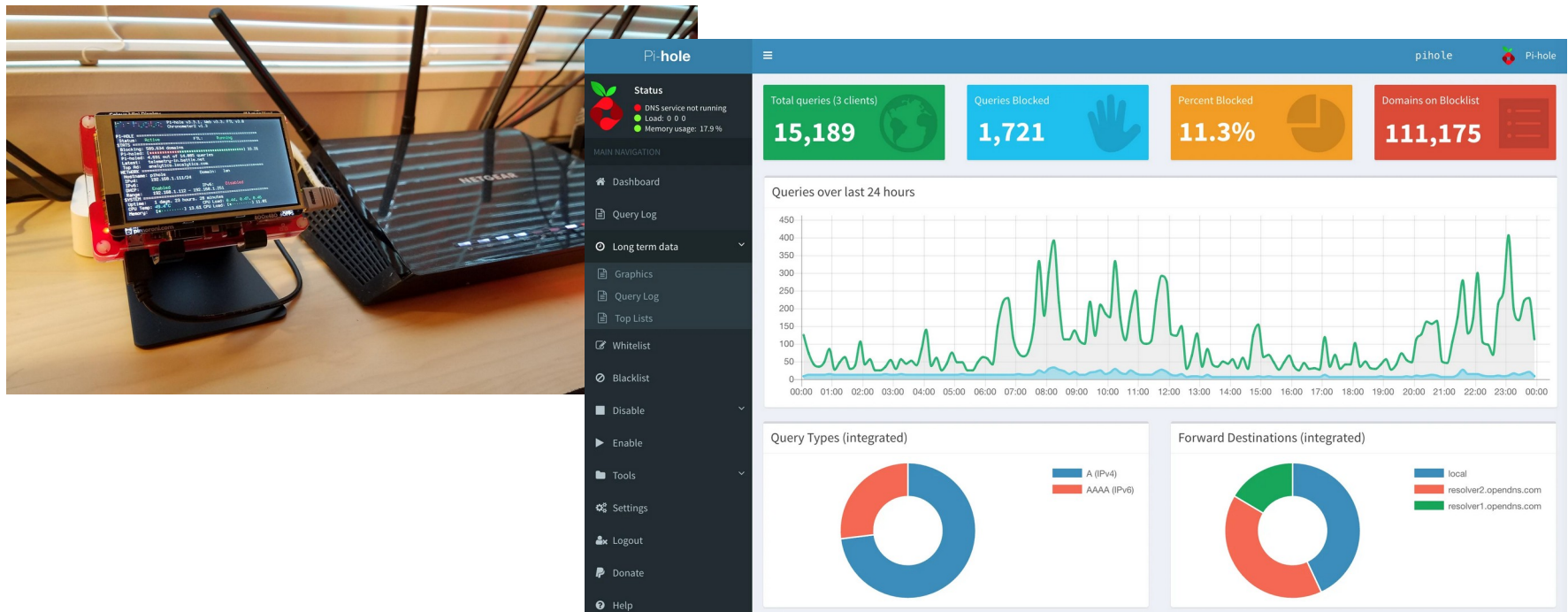
Typen von Einträgen

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

- DNS ist ein durchaus kritischer Dienst
- Da er nur **UDP** verwendet, ist er häufig Angriffsziel:
 - DNS ID Hacking: Anfragen werden über IDs geschützt, d.h. man der Client erwartet nicht nur die Auflösung, sondern auch noch eine spezielle ID. Wenn diese nicht vom Netz abgegriffen werden kann, so muss man sie erraten
 - DNS spoofing: Hier beantwortet ein falscher DNS-Server die Anfrage. Hier muss die ID verwendet werden. Auch wird die falsche IP, also die des eigentlich richtigen Servers angegeben (was von den Providern zu unterbinden ist)
 - DNS Cache Poisoning: Hier wird versucht, einen eigentlich korrekten DNS-Server zu „verseuchen“. Idee ist, den Cache falsch zu füllen.

DNS-Filter

- DNS-Anfragen können mit einem Proxy gefiltert werden, um z.B. unerwünschte Anfragen zu unterdrücken
- Projekt Pi-Hole (Raspberry Pi wird zum DNS-Proxy, und leitet nur gewünschte DNS Anfragen weiter



FH Aachen
Fachbereich 9 Medizintechnik und Technomathematik
Prof. Dr.-Ing. Andreas Terstegge
Straße Nr.
PLZ Ort
T +49. 241. 6009 53813
F +49. 241. 6009 53119
Terstegge@fh-aachen.de
www.fh-aachen.de