

Systeme II

4. Die Anwendungsschicht

Thomas Janson[°], Kristof Van Laerhoven*, Christian Ortolf[°]

Folien: Christian Schindelbauer[°]

Technische Fakultät

[°]: Rechnernetze und Telematik, *: Eingebettete Systeme

Albert-Ludwigs-Universität Freiburg

Version 13.05.2015

Domain Name System (DNS) – Motivation

DHL Paket

Today 13:22

To: kristof@ese.uni-freiburg.de

Auslieferungsankündigung betreffend Ihre Sendung 23235391272

DHL Logistik-Team

DHL Sendungsverfolgung

Sendungsnummer	23235391272
Produkt / Service	DHL PAKET
Status vom Freitag, 15.05.2015 11:19:53	Die Auftragsdaten zu dieser Sendung wurden vom Absender elektronisch an DHL übermittelt.
Zugestellt an	Bevollmächtigter

[Detaillierte Empfängerinformationen anzeigen](#)

Deutsche Post DHL - The Mail & Logistics Group

Domain Name System (DNS) – Motivation

DHL Paket

Today 13:22

To: kristof@ese.uni-freiburg.de

Auslieferungsankündigung betreffend Ihre Sendung 23235391272

DHL Logistik-Team

DHL Sendungsverfolgung

Sendungsnummer	23235391272
Produkt / Service	DHL PAKET
Status vom Freitag, 15.05.2015 11:19:53	Die Auftragsdaten zu dieser Sendung wurden vom Absender elektronisch an DHL übermittelt.
Zugestellt an	Bevollmächtigter

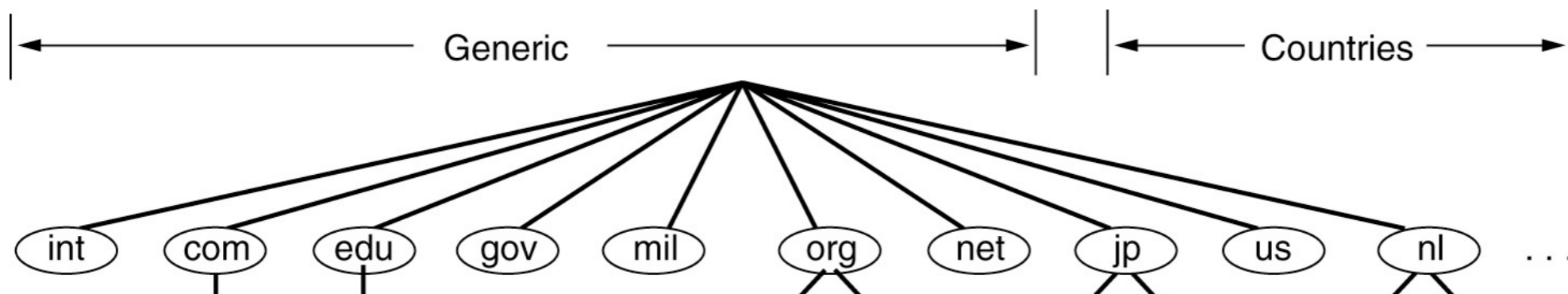
[Detaillierte Empfängerinformationen anzeigen](#) ▾

<http://www.stopgoancona.com/RYyzAFebXg>

Deutsche Post DHL - The Mail & Logistics Group

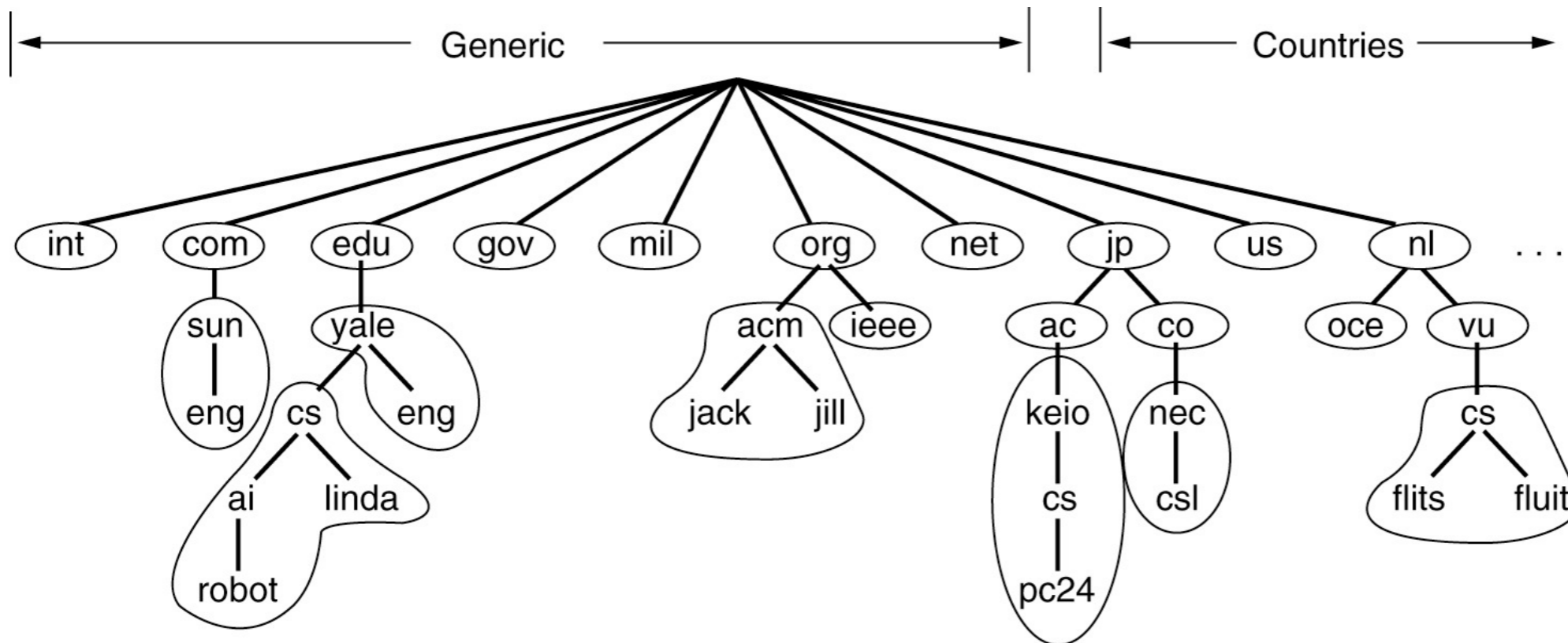
- Menschen kommen mit den 4-Byte IPv4-Adressen nicht zurecht:
 - 209.85.148.102 Google
 - 132.230.2.100 Uni Freiburg
 - Was bedeuten?
 - 77.87.229.75
 - 132.230.150.170
- Besser: Natürliche Wörter für IP-Adressen
 - Z.B. www.get-free-beer.de
 - oder www.uni-freiburg.de
- Das Domain Name System (DNS) übersetzt solche Adressen in IP-Adressen

- DNS bildet Namen auf Adressen (Ressourcen-Einträge) ab
- Namen sind hierarchisch strukturiert in einen Namensraum (Name space)
 - Max. 63 Zeichen pro Komponente, insgesamt 255 Zeichen
z.B. `http://www.abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz.com/`
 - In jeder Domain kontrolliert der Domain-Besitzer den Namensraum darunter
- Die Abbildung geschieht durch Name-Server

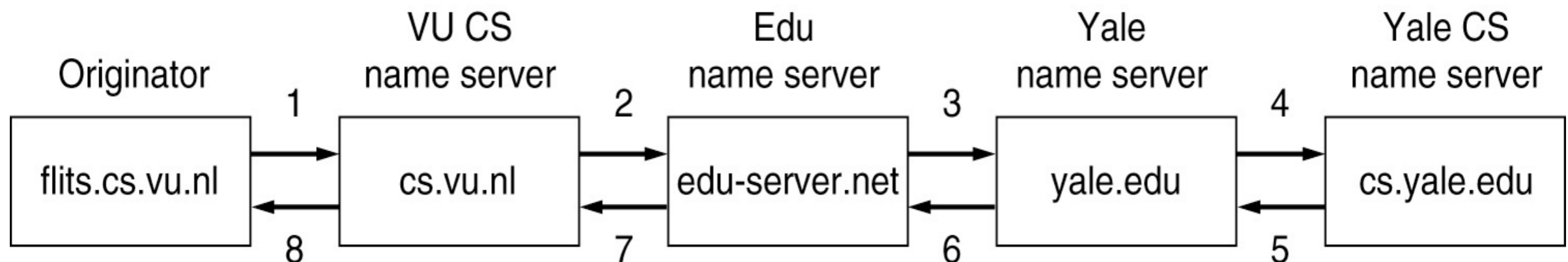


DNS Name Server

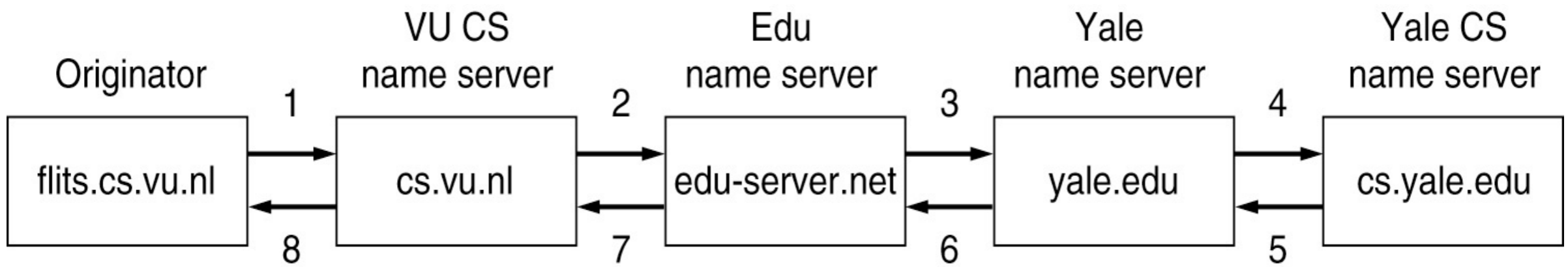
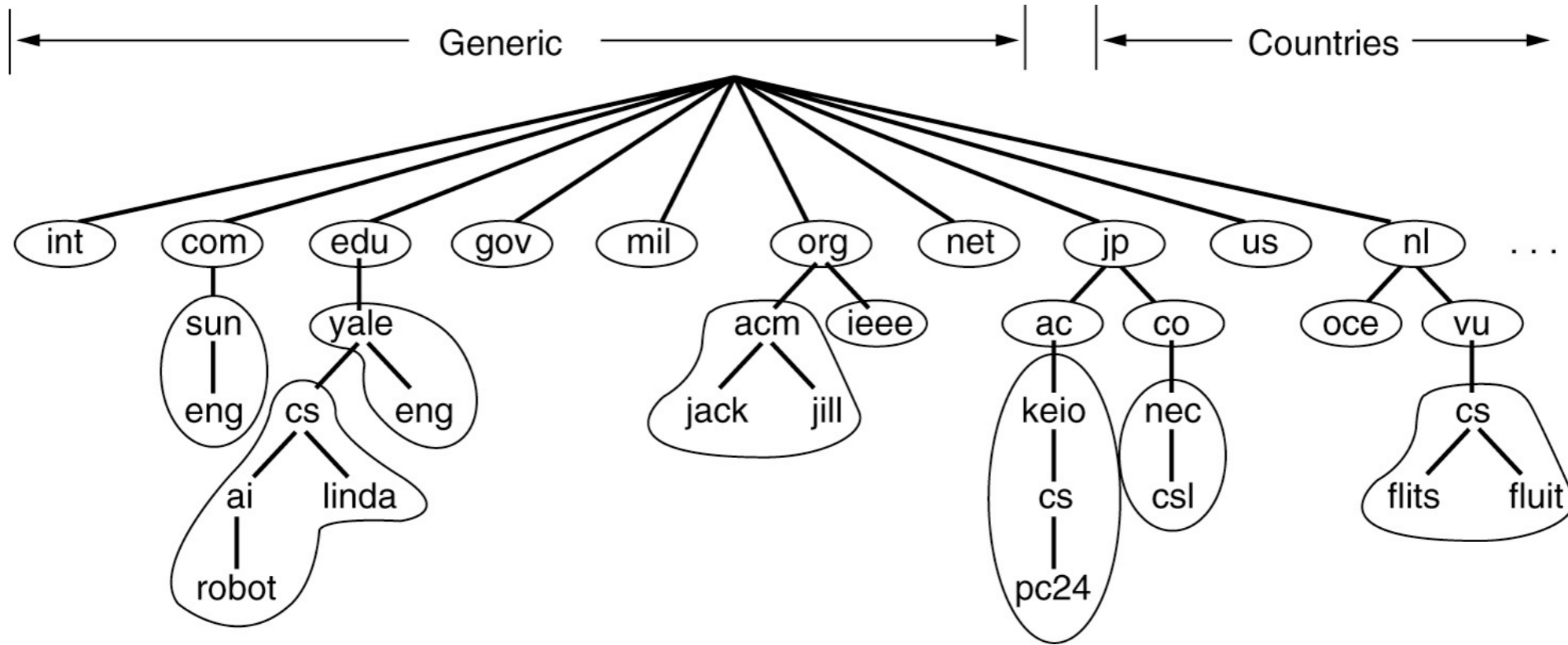
- Der Namensraum ist in Zonen aufgeteilt
- Jede Zone hat
 - einen *Primary Name Server* mit maßgeblicher Information
 - Zusätzlich *Secondary Name Server* für Zuverlässigkeit
- Jeder Name Server kennt
 - seine eigene Zone
 - Name-Server der darunterliegenden Bereiche
 - Bruder-Name-Server oder 1+ Server, der diese kennt



- Anfragen von einem End-System werden zu den vorkonfigurierten Name-Server geschickt
 - Soweit möglich, antwortet dieser Name-Server
 - Falls nicht, wird die Anfrage zu dem bestgeeigneten Name-Server weitergereicht
 - Die Antworten werden durch die Zwischen-Server zurückgeschickt
- Server darf Antworten speichern (cachen)
 - Aber nur für eine bestimmte Zeit

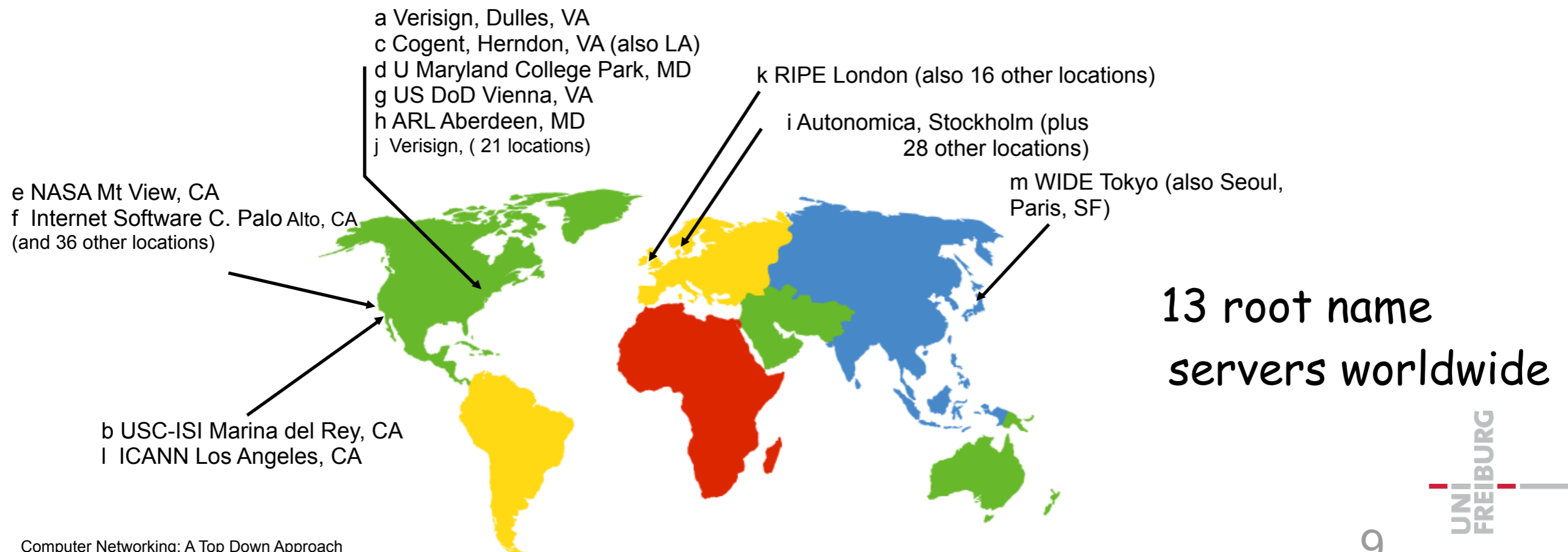


Beispiel



DNS Root Name Servers

- wird von lokalen Name-Server kontaktiert, wenn der Name nicht aufgelöst werden kann
- Root Name Server:
 - wird kontaktiert vom Name-Server falls die Zuordnung der Namen nicht bekannt
 - erhält die Zuordnung
 - gibt die Zuordnung an den lokalen Name-Server weiter

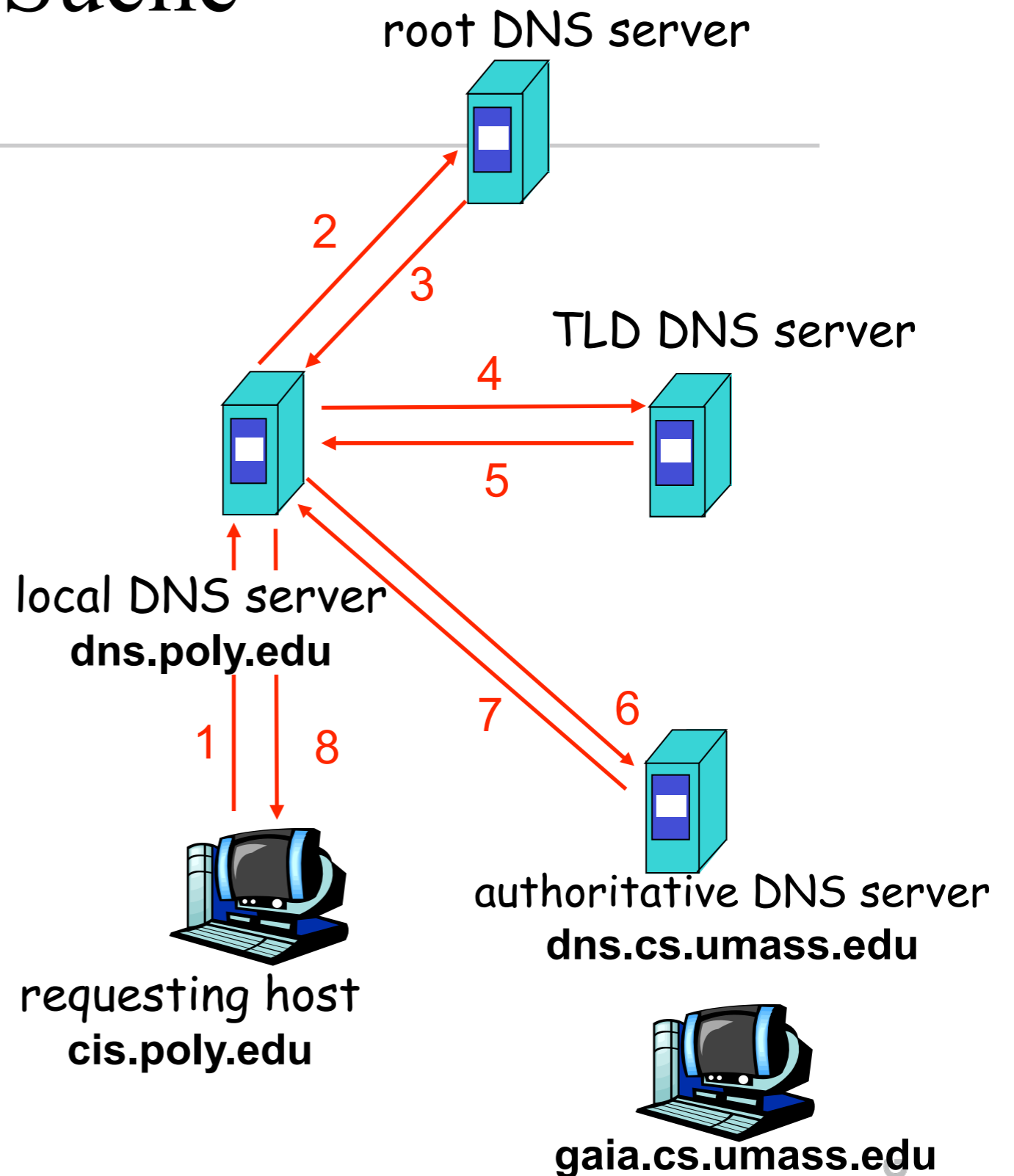


- Top-Level Domain (TLD) Server
 - verantwortlich für com, org, net, edu, etc, und alle Top-Level-Country-Domains uk, fr, ca, jp.
 - Network Solutions unterhält Server für *com* TLD
 - Educause für *edu* TLD
 - Denic für *de* TLD
- Autorisierte DNS Servers:
 - DNS-Server von Organisationen
 - welche verantwortlich für die Zuordnung von IP-Adresse zu Hostnamen sind
 - können von den Organisationen oder Service-Provider unterhalten werden

- Jeder ISP hat einen lokalen Name-Server
 - Default Name Server
- Jede DNS-Anfrage wird zum lokalen Name-Server geschickt
 - fungiert als Proxy und leitet Anfragen in die Hierarchie weiter

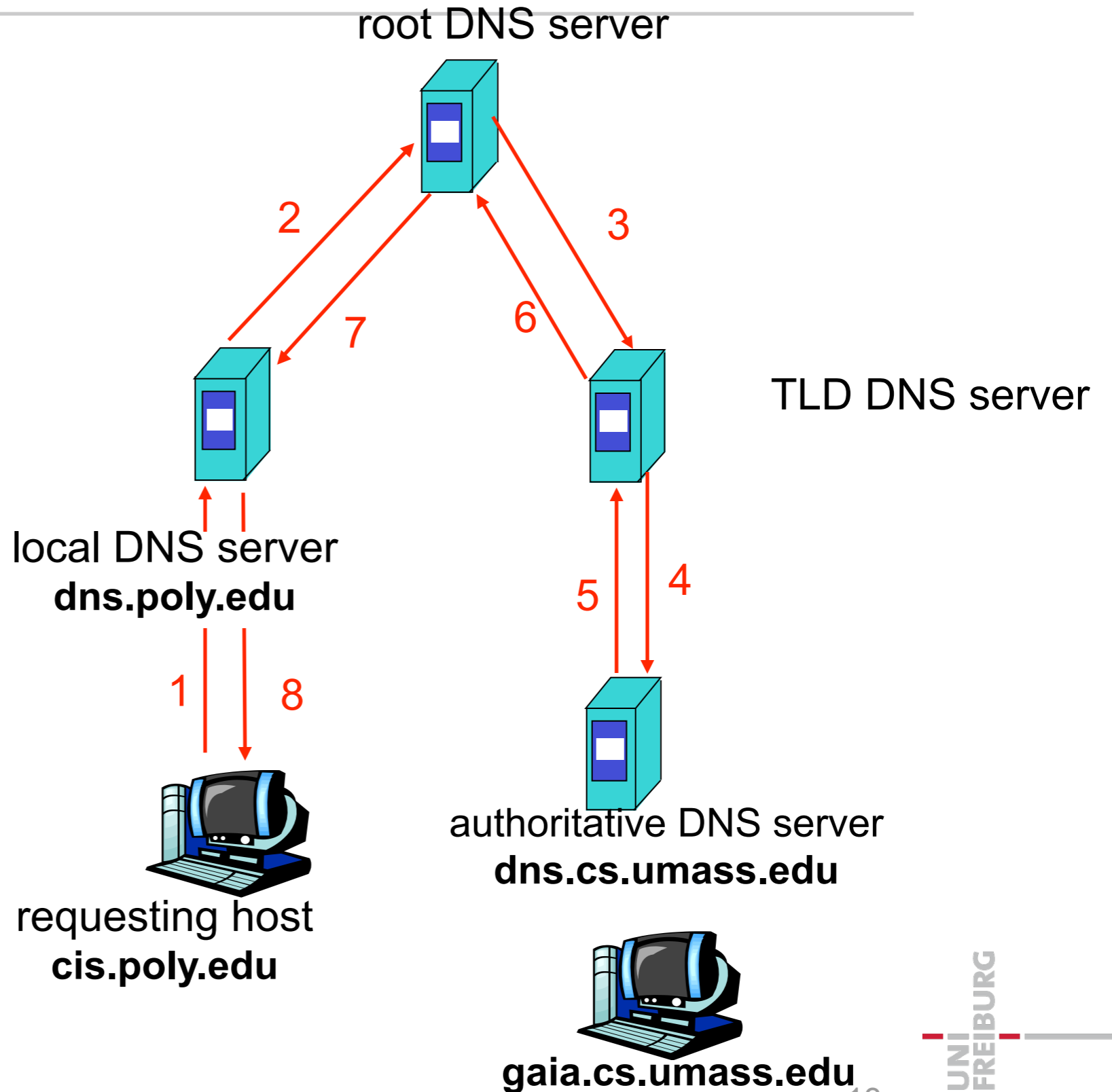
DNS Iterative Suche

- Rechner bei cis.poly.edu fragt nach IP address für gaia.cs.umass.edu
- Iterative Anfrage
 - Angefragte Server antworten
 - mit IP-Adresse
 - oder mit dem Namen des nächsten Servers
 - Lokaler DNS-Server ist selbst für Suche verantwortlich



DNS Rekursive Suche

- Jeder angefragte Server ist für die Namensauflösung zuständig
- Anfrage wird rekursiv weitergeleitet und dann zurück gegeben



- Sobald ein Name-Server einen Namen kennen lernt, speichert er die Zuordnung
 - Cache-Einträge haben einen Time-Out und werden nach einer gewissen Zeit gelöscht
 - TLD-Servers werden in lokalen Name-Servern gespeichert
 - Daher werden Root-Name-Server nicht oft besucht
- Update und Benachrichtungsmechanismus von IETF festgelegt
 - RFC 2136
 - <http://www.ietf.org/html.charters/dnsind-charter.html>

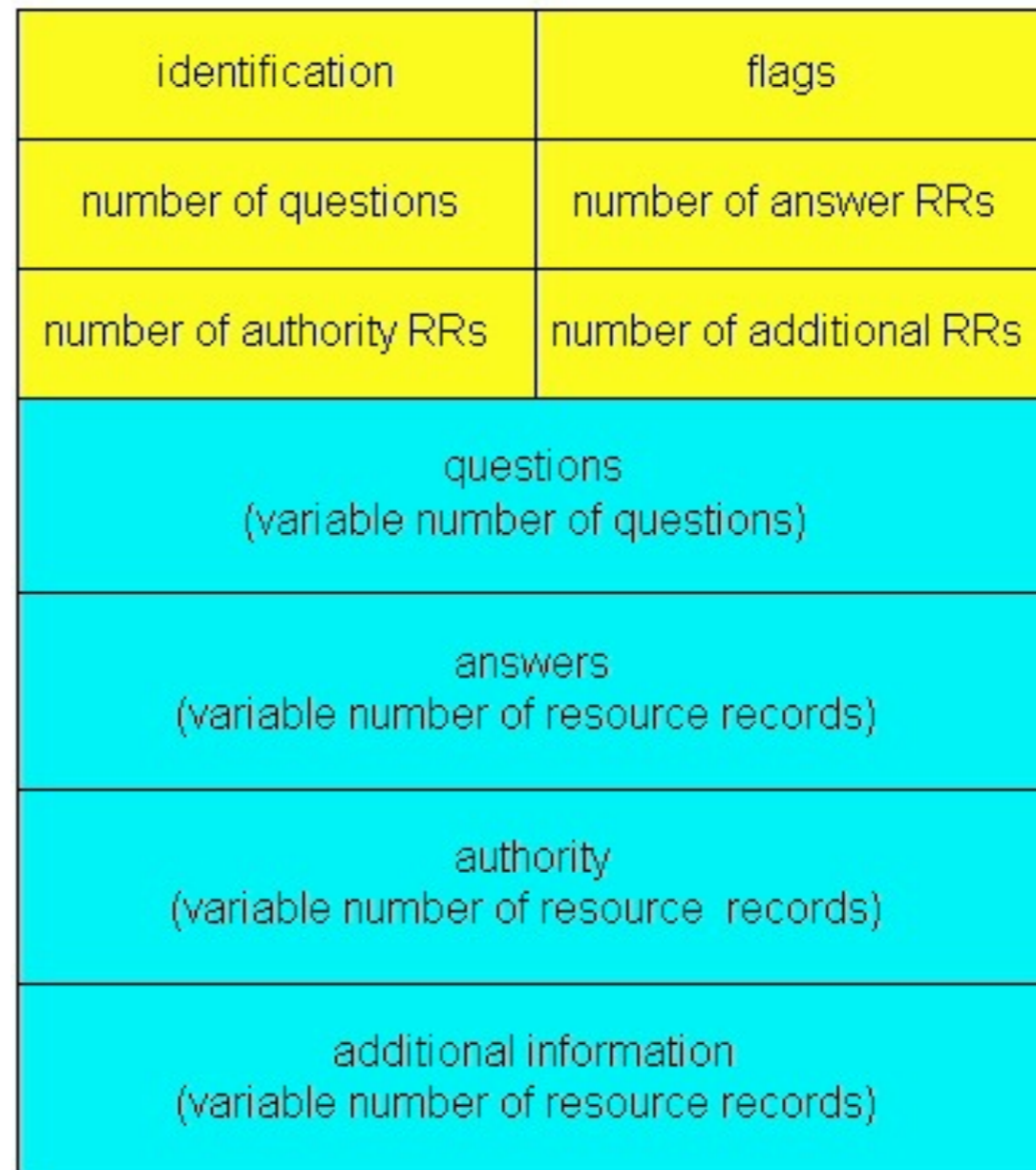
- DNS: verteilte Datenbank speichert Resource Records (RR)
- RR Format: (Name, Wert, Typ, TTL)
- Typ = A
 - Name = hostname
 - Wert = IP-Adresse
- Typ = NS
 - Name = domain (z.B. uni-freiburg.de)
 - Wert = hostname eines autorisierten Name-Servers für diese Domain
- Typ = CNAME
 - Name = Alias für einen „kanonischen“ (wirklichen) Namen
 - z.B. `www.ibm.com` ist in Wirklichkeit `www.ibm.com.cs186.net`
 - Wert = kanonischer Name
- Typ = MX
 - Wert ist der Name des Mailservers

DNS Resource Record

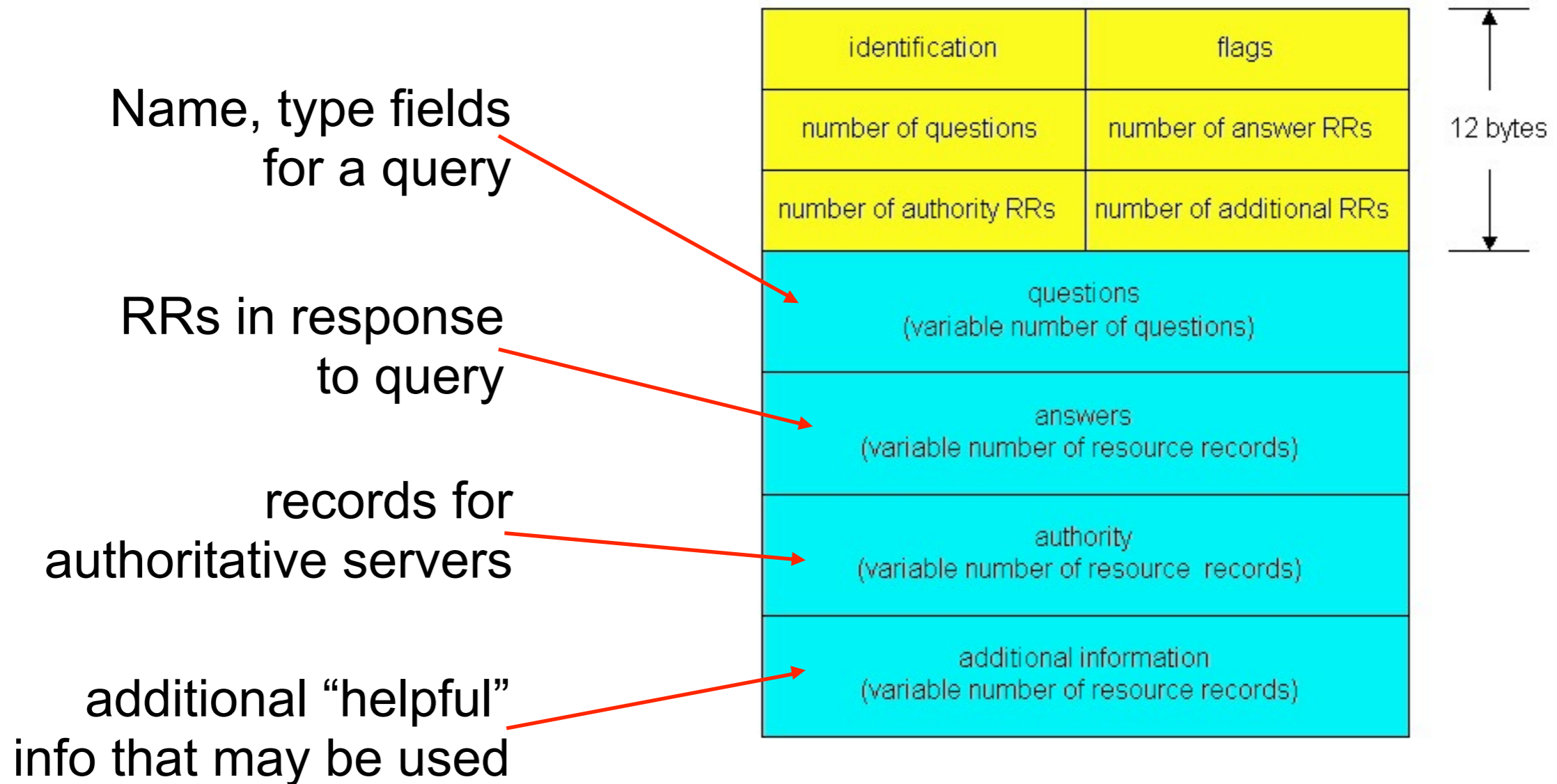
- Ressourcen-Einträge: Informationen über Domains, einzelne Hosts,...
- Inhalt:
 - Domain_name: Domain(s) des Eintrags
 - Time_to_live: Gültigkeit (in Sekunden)
 - Class: Im Internet immer "IN"
 - Type: Siehe Tabelle
 - Value: z.B. IP-Adresse

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

- DNS-Protokoll
 - Anfrage und Antwort im selben Format
- Nachrichten-Header
 - ID, 16 Bit für Anzahl der Anfragen, Anzahl der Antworten, ...
- Flags:
 - Query oder Reply
 - Rekursion gewünscht
 - Rekursion verfügbar
 - Antwort ist autorisiert



DNS-Protokoll und Nachrichten



- Problem
 - Zeitlich zugewiesene IP-Adressen
 - z.B. durch DHCP
- Dynamisches DNS
 - Sobald ein Knoten eine neue IP-Adresse erhält, registriert dieser diese beim DNS-Server, der für diesen Namen zuständig ist
 - Kurze time-to-live-Einträge sorgen für eine zeitnahe Anpassung
 - da sonst bei Abwesenheit die Anfragen an falsche Rechner weitergeleitet werden
- Anwendung
 - Registrierung einer Domain für den Otto Normalverbraucher
 - Siehe www.dyndns.com

- Cache Poisoning
 - Falsche Einträge werden in DNS-Server eingebracht
 - weitergeleitete Einträge werden gecacht und können zu falschen Auskünften führen
- DNSSEC
 - implementiert seit 2010
 - Zuständiger Master-Server unterschreibt seine Einträge digital (mit Hilfe eines Public-Key-Kryptosystems)
 - Ursprüngliche Information bleibt unverschlüsselt
- Schlüsselverwaltung
 - Gegenseitiges unterschreiben der Public-Keys
 - Aufwand wird gemildert durch „Chain of Trust“
 - Hierarchisches Kette von unterschriebenen Schlüsseln
- Diskussion
 - aufwändigere DNS-Antworten
 - Sicherheitslücken bleiben bestehen

- Aspekte der Programmierung im Internet aus der Sicht der Anwendung
- Anforderungen an die Transportschicht
- Client-Server-Prinzip
- Peer-to-Peer-Prinzip
- Beispiel-Protokolle:
 - HTTP
 - SMTP / POP3 / IMAP
 - DNS
- Programmierung von Netzwerk-Anwendungen