Zur Info: Klausurtermin

- Semestralklausur
  - Donnerstag, 26.07.2018
  - 14:00 bis 15:30 Uhr im Hauptgebäude der LMU
  - Einlass ab 13:30 Uhr
  - Anmeldung über UniWorX nötig
- Nachholklausur
  - Gegen Ende der vorlesungsfreien Zeit
  - Genauer Termin wird noch bekannt gegeben

Kapitel 2:
Namen und Adressen

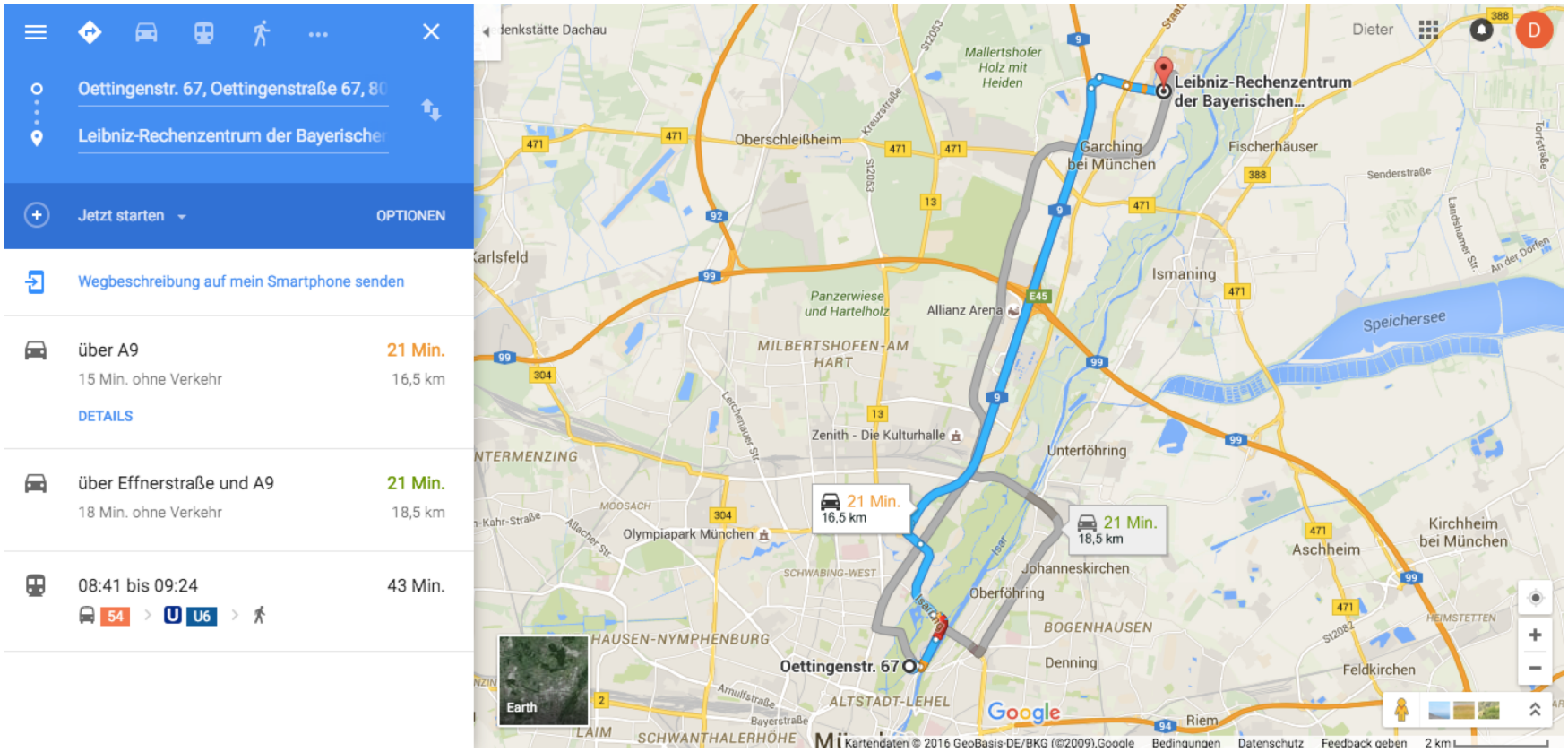
MNM
TEAM

Inhalt von Kapitel 2

- **Querschnittsthema** „Namen und Adressen“
- Namen bzw. Adressen können in allen Schichten und Protokollen zum Einsatz kommen.

1. Allgemeines
2. IPv4 Adressen
3. DNS – Domain Name System

Namen und Adressen



Kapitel 2.1
Allgemeines zu Namen und Adressen

Motivation/Grundproblem

- **WH**: In einem verteilten System wird mittels Austausch von Nachrichten kommuniziert.
- **Grundproblem**:
  Für die Kommunikation ist es notwendig, dass die *Adressen* der Kommunikationspartner bekannt sind bzw. diese *adressiert* werden können
- Zusätzlich:
  - Aus *Adressen* müssen *Pfade* bzw. *Wege* ableitbar sein
  - Zwischenstationen sollten Nachrichten mit gegebener Adressierung so weiterreichen, dass diese möglichst effektiv an ihr Ziel gelangen.

Begriffsklärung

- **Adressen** dienen der Identifizierung von Netzkomponenten oder Diensten
- Adressen müssen von von Maschinen (Computern) effizient verarbeitet werden können
- (Mnemonische) **Namen** sind solche, die Menschen sich gut merken können
- *Namens-* oder *Adressraum* ist eine Menge von eindeutigen Namen bzw. Adressen, die uns in einem bestimmen Format zur Kommunikation in einem Kontext zur Verfügung stehen

Eigenschaften

- (Mnemonische) Namen
  - dienen der Bequemlichkeit menschlicher Nutzer
  - mehrere Inkarnationen logisch identischer Objekte
  - Objekten können ortsunabhängig Namen behalten
  - Bedeutung oft kontextabhängig
  - strukturiert oder flach
- Adressen
  - dienen der effizienten maschinellen Verarbeitung
  - werden für Routing/Wegewahl verwendet
  - strukturiert oder flach

Adressbildung

- Struktur
  - uniform global (durchlaufende Nummerierung) (Bsp.: Ethernet-Adressen)
  - hierarchisch (Bsp.: Telefonnummern)
- Umfang des Adressraums
  - groß genug: ermöglicht permanente Zuordnung, erfordert große Header
  - Zu klein: Mehrfachverwendung erfordert dynamische Vergabestrategie (Bsp.: DHCP)
- Codierung
  - variable Namensfelder: erweiterbar
  - feste Namensfelder: effizient/einfach zu implementieren

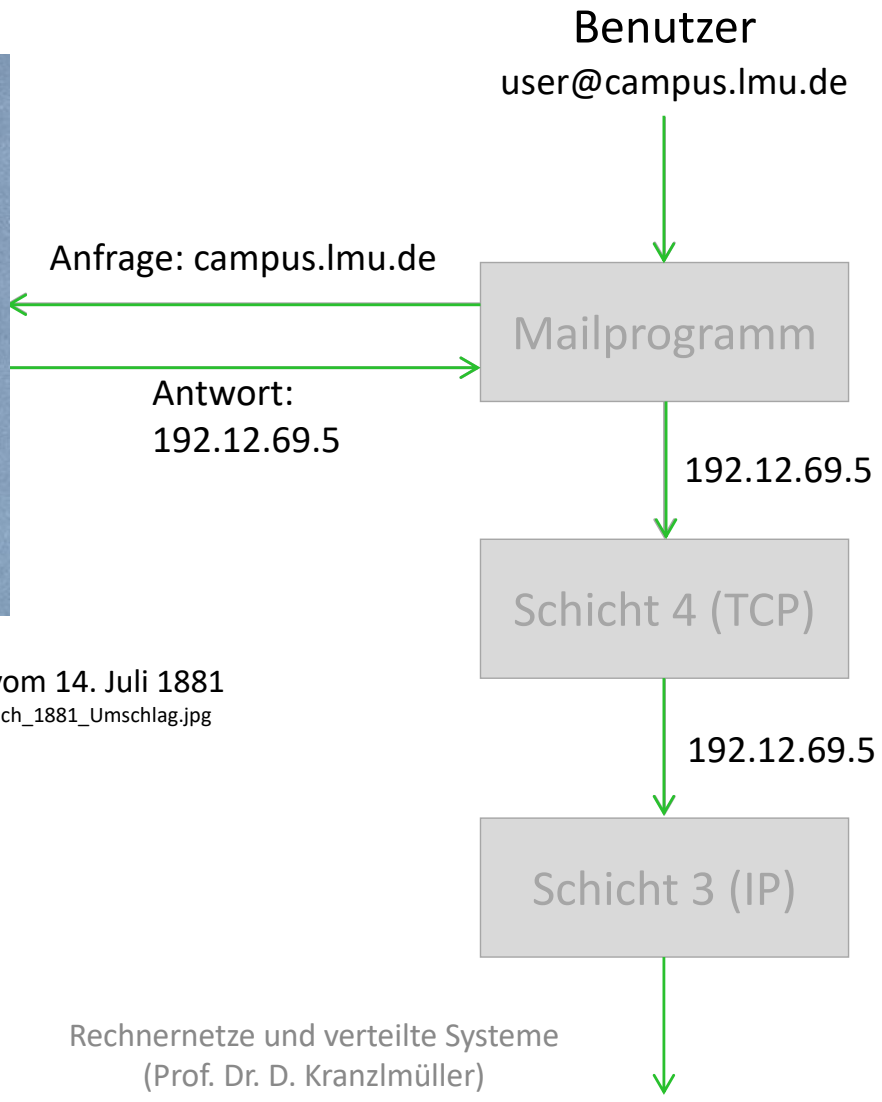
Lokalisierung von Objekten

- **Namensauflösung**: Adressfindung der Objekte, für die ein Name steht
- Zwei Ansätze:
  - Namen werden durch separaten Dienst z.B. mit Hilfe von Zuordnungstabellen abgebildet
  - Adresse ist aus der Namensstruktur ableitbar: <Prozessname>:=<Netz>.<Subnetz>.<Host>.<ID>
- Im Internet:
  Namensauflösung via DNS ➔ Kapitel 2.3

Beispiel: Namensauflösung Mail

(stark vereinfacht)

Umschlagseite des Berliner Telefonbuchs vom 14. Juli 1881
https://commons.wikimedia.org/wiki/File:Berliner_Telefonbuch_1881_Umschlag.jpg



Kapitel 2.2
IPv4-Adressen

Adressen im Internet

Einordnung

- Internet Protokoll (IP) ist zentrales Protokoll des Internets
- Es implementiert die Funktionalität der Vermittlungsschicht (Schicht 3) (➔ Kapitel 4)
- **IP-Adressen** sind Bestandteil des Internet Protokolls.
- In diesem Kapitel: IPv4 = Version 4 des IP (IPv6 ➔ Kapitel 4).
- IPv4 Adressen sind **32-bit Binärzahlen**

Grundidee und Vergabe (1/2)

- Jeder Host bekommt eindeutige IP-Adresse
  - Strikt genommen bekommen nicht Hosts, sondern Netzschnittstellen IP-Adressen.
  - Ein Host hat oft mehrere Netzschnittstellen hat (z.B. bei Routern der Fall)
  - Im Heimnetz: Hinter einer Netzschnittstelle verbergen sich mehrere Hosts (➔ NAT).

- Jeder Host (mit IP-Adresse) kann jederzeit an jeden anderen Host (mit IP-Adresse) ein IP-Paket verschicken

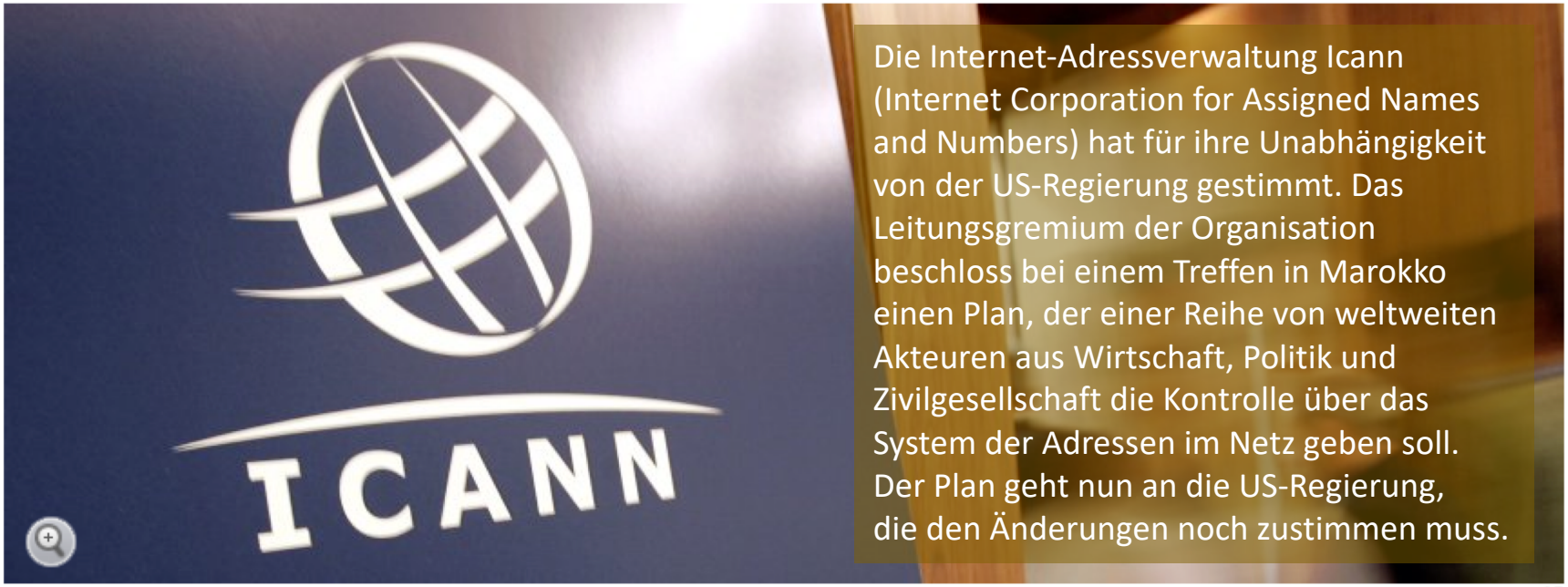
Grundidee und Vergabe

- IPv4-Adressen werden hierarchisch verwendet.
  - IPv4-Adressen bestehen aus Netzteil (Netz ID), der das Netz adressiert, und Hostteil (Host ID), der den Host adressiert
- Einzelne IP-Adressen haben Sonderbedeutungen.

- Internationale Vergabe durch die IANA (Internet Assigned Numbers Authority)
  - Delegiert an nationale Organisationen.
  - Abteilung der ICANN (Internet Corporation for Assigned Names and Numbers)
  - Buchhalter für die Registrierungen

Politik und ICANN

Internet-Adressen: Icann sagt sich von US-Abhängigkeit los



Icann-Logo

Die Icann ist die Hüterin über die Adressen im Internet. Bisher stand die Adressverwaltung unter der Aufsicht des US-Handelsministeriums. Jetzt stimmte das Gremium für neue Kontrollmechanismen.

http://www.spiegel.de/netzwelt/netzpolitik/icann-sagt-sich-von-us-abhaengigkeit-los-a-1081731.html

Historischer Hintergrund

- **Ursprünglich**: hauptsächlich Universitäten und Forschungseinrichtungen brauchen Internetzugang
- **Wandel**: Internet als Massenkommunikationsnetz
  ➔ 2^{32} IP-Adressen werden nicht (lange) reichen
- **Kurzfristig**: Entwicklungen und Maßnahmen, um mit den bestehenden IPv4-Adressen auszukommen (NAT, CIDR, ...)
- **Langfristig**: Migration zu IPv6 (128-bit Adressen)

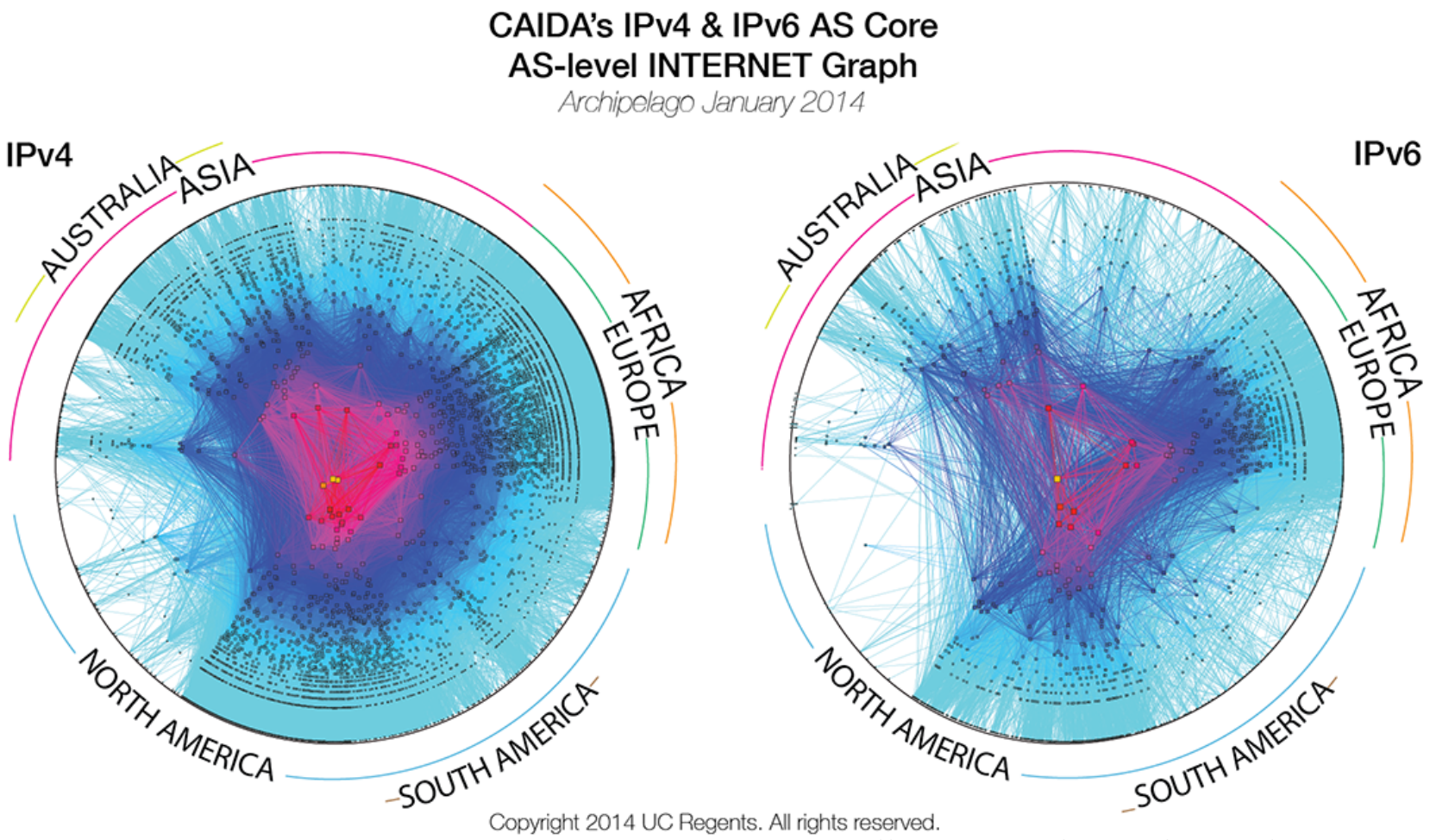
Historische Entwicklung (1/2)

- 1981: Mit RFC 791 wird IPv4 zum Standard.
- 1981-1993: Klassenbasierte Adressierung (engl.: Classful Networking) – Es gibt genug IPv4 Adressen.
- 1993: RFC 1517-1520: CIDR (engl.: Classless Inter-Domain Routing) – Ermöglicht sparsamere Vergabe von Adressblöcken.
- 1994/1996: Mit RFCs 1597 und 1918 werden private Adressblöcke eingeführt, die insbesondere in Verbindung mit NAT (engl.: Network Address Translation) verwendet werden.

Historische Entwicklung (2/2)

- 1994: Arbeit an IPv6 beginnt.
- 1998: Mit RFC 2460 wird IPv6 zum Standard (Einsetzung erfolgt nur langsam).
- 2011: Die IANA (engl.: Internet Assigned Numbers Authority) gibt ihren letzten IPv4-Adressblock aus.
- 2011/2012: World IPv6 Day und World IPv6 Launch Day (Publicity Events)
- März 2014: 17,4% aller Netze der globalen Routing Tabelle unterstützen IPv6.

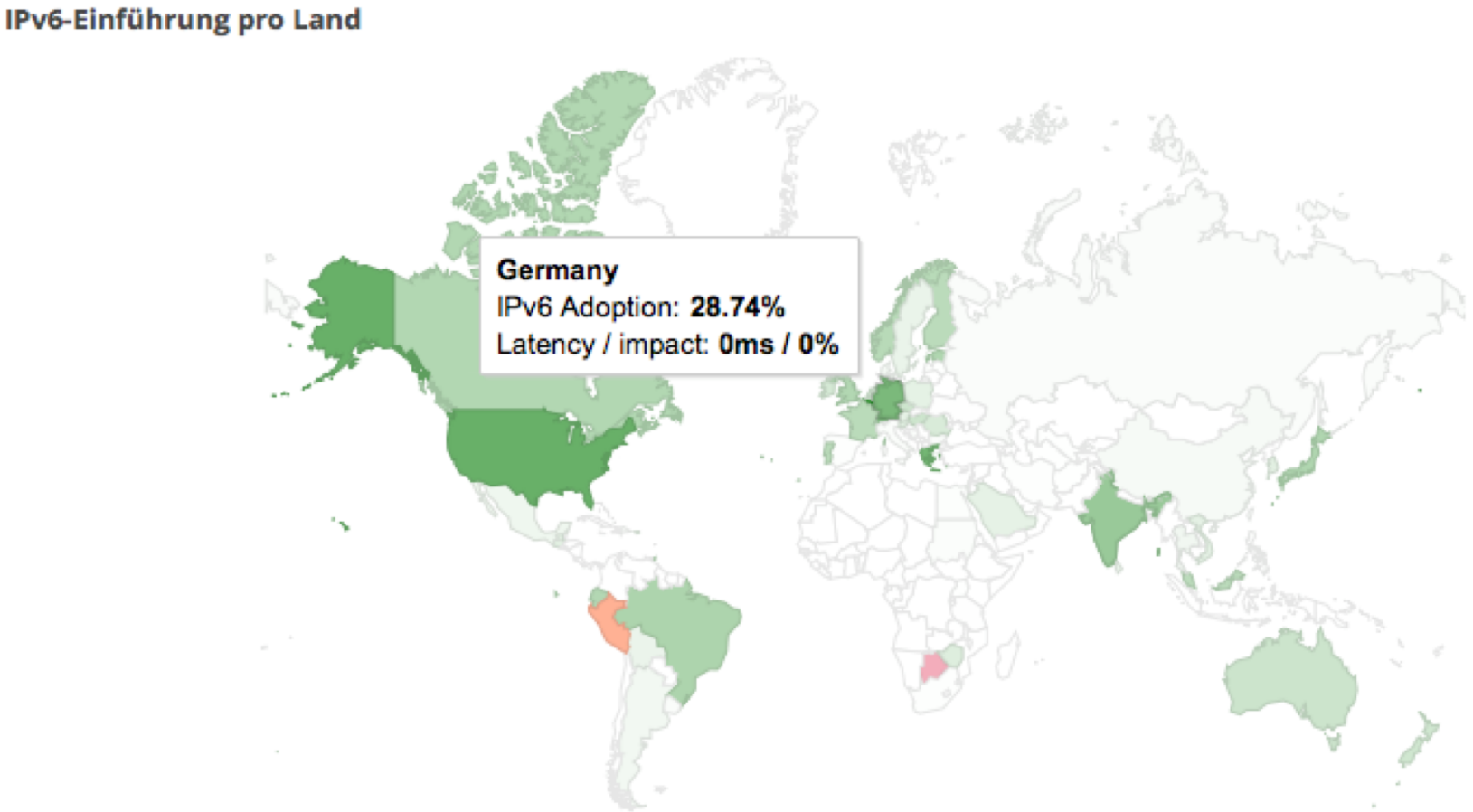
Karte des Internet (2014)



https://www.caida.org/research/topology/as_core_network/2015/

IPv6 Einführung pro Land

https://www.google.de/ipv6/statistics.html#tab=per-country-ipv6-adoption



Notation von IPv4-Adressen

- Durch Punkte getrennte, byteweise Dezimalschreibweise: p.q.r.s
- wobei p,q,r,s Dezimalzahlen zwischen 0 und 255 sind.
- Beispiel: „208.77.255.0“

- Binärzahl-Darstellung oft hilfreich (Stichwort: Netzmasken)

Sonderadressen

p.q.r.s:

- alles 0: dieser Host
- alles 1: Broadcast innerhalb des lokalen Netzes
- 127.*.*.*: Loop-Back-Adressen (Schleifentest)

Später: 2 spezielle Adressen

- Netzadresse:
  niedrigste Adresse (Host-ID = alles 0)
- Broadcast-Adresse:
  höchste Adresse (Host-ID = alles 1)

Klassenbasierte Adressierung (Engl.: Classful Networking)

Grundidee:

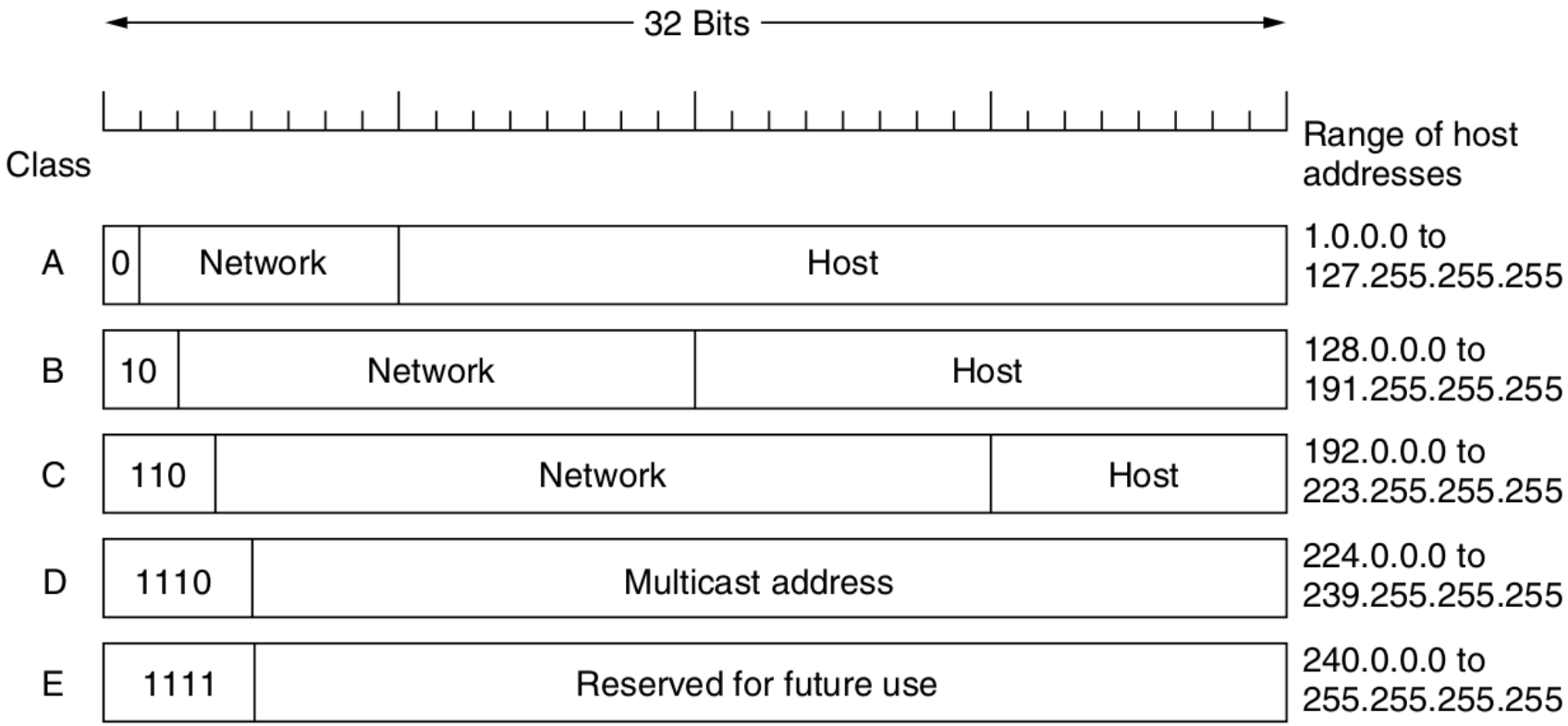
- Einteilung in Klassen anhand des Verwendungszwecks:
  - Netzgrößen für Unicast (A,B,C)
  - Multicast Network (D)
  - Future and Experimental Use (E)
- Grenze zwischen Netz-Teil und Host-Teil verläuft entlang der Byte-Grenzen ➔ Softwareimplementierung
- Netz-Teil wird in Präfix und Netz-ID unterteilt
  - Erlaubt schnelle Erkennung der Klasse anhand weniger Bits
  - Schnelle Routing-Entscheidungen anhand Klasse und Netz-ID

Klassenbasierte Adressierung (Engl.: Classful Networking)

https://de.wikipedia.org/wiki/Netzklasse

Klasse	Präfix	Länge Netz ID	Länge Host ID	Anzahl Netze	Hosts pro Netz
A	0	7 bit	24 bit (3 byte)	126	16 777 214
B	10	14 bit	16 bit (2 byte)	16 382	65 534
C	110	21 bit	8 bit (1 byte)	2 097 152	254
D	1110	Verwendung für Multicast-Anwendungen			
E	1111	Reserviert (für zukünftige Zwecke)			

Klassenbasierte Adressierung (Grafik)



Quelle: Tanenbaum, Computer Networks 5th Edition

Klassenbasierte Adressierung Grundproblem

- Adressen werden in Blöcken vergeben (z.B.: alle Adressen mit einer gegebenen Netz-ID)
- Wird z.B. ein Klasse B Netz an eine Organisation vergeben welche deutlich weniger als 65000 Hosts besitzt, so bleiben viele Adressen ungenutzt.
- (Oft reicht bereits die Erwartung, dass 254 Hosts einmal nicht reichen könnten, für die Anforderung eines Klasse B Adressblocks.)
- Es gibt nur 16382 Klasse B Netze.
- Lösung: Netz IDs mit variabler Länge → CIDR

CIDR (Engl.: Classless Inter-Domain Routing)

- Mit RFC 1517 bis 1520 ab 1993 in Verwendung.
- Grundidee: Die Grenze zwischen Netz-Teil und Host-Teil verläuft fließend.
  => Routing-Protokolle müssen die Länge der Netz-ID (Netzpräfix) zusätzlich zur Adresse übertragen.
- Verwendung von Subnetz-Masken
- Notation: <IP Adresse>/<Präfixlänge>

- Beispiel: 192.168.121.0/26
  (die ersten 26 Bit sind Netz-ID, der Rest Host-ID)

Private IP-Adressen (1/2)

- I.d.R. vergeben ISPs (engl.: Internet Service Providers) an Privatkunden oder kleine Firmen nur eine einzige öffentliche IP Adresse (unabhängig davon wie viele Hosts diese in ihrem LAN anschließen).
- Innerhalb ihres LANs (engl.: Local Area Network) verwenden die Hosts sogenannte private IP-Adressen (nur innerhalb des LANs eindeutig)

Private IP-Adressen (2/2)

- Folgende Adressblöcke sind als privat reserviert:
  - 10.0.0.0/8 (Klasse A Adressblock)
  - 172.16.0.0/12 (16 Klasse B Adressblöcke)
  - 192.168.0.0/16 (256 Klasse C Adressblöcke)

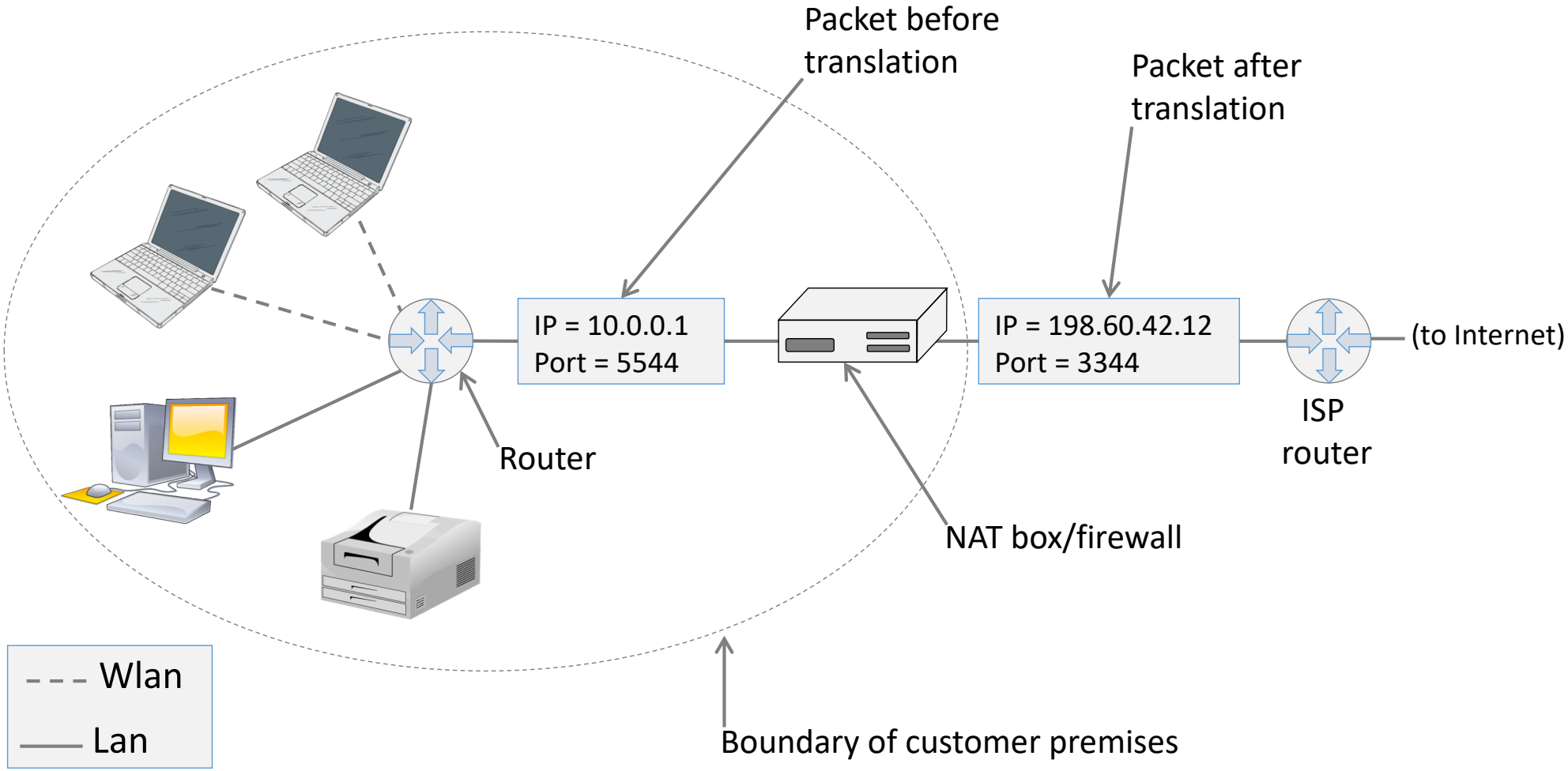
- Private Adressen werden nicht im Internet vermittelt
- Pakete mit privaten Adressen als Ziel oder Absender werden von Routern verworfen

NAT (Network Address Translation)

(Vergleiche auch „Kapitel 1.4: Ein Einführendes Beispiel“)

- Bevor Router ein Paket aus dem privaten LAN ins Internet weiterleitet, wird Absenderadresse in öffentliche IP-Adresse geändert
  ➔ „*Address Translation*“
- Router merkt sich die Änderung der Adresse
- Zusätzlich zur Adresse wird auch der verwendete Port gemerkt (siehe Sockets ➔ Kapitel 3)
- Auf „Rückweg“ erfolgt umgekehrte Übersetzung.

NAT/Mascquerading (als Grafik)



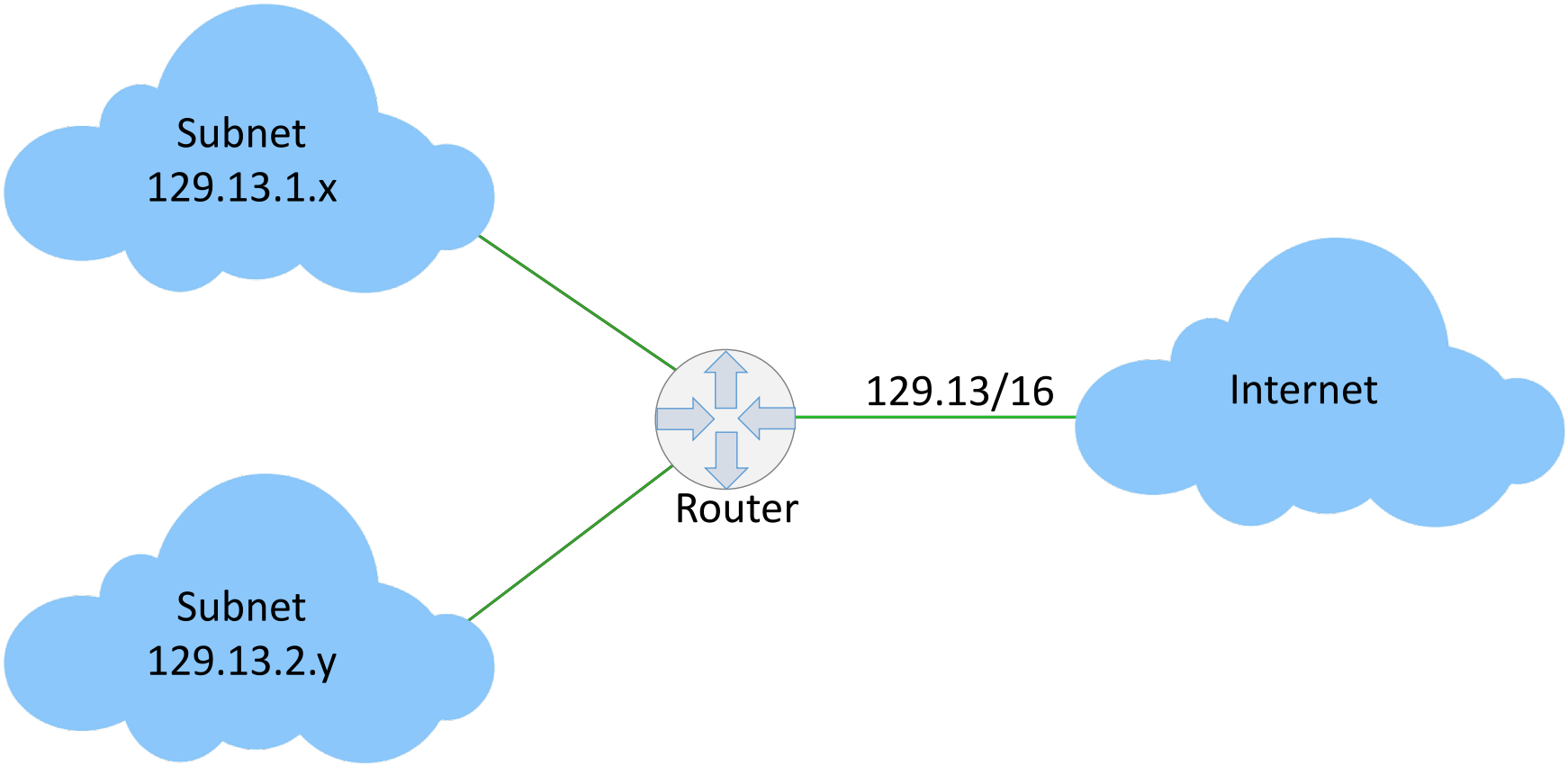
Subnetting

- Sowohl bei klassenbasierter Adressierung, als auch bei CIDR
- Grundidee: Host-Teil eines Adressblocks wird weiter unterteilt in Subnetz-ID-Teil und Host-ID-Teil.

Netz ID	Host ID	
Netz ID	Subnetz ID	Host ID

- Eine Organisation kann mit einem einzigem Adressblock mehrere eigene Netze bedienen

Subnetting (als Grafik)



Beispiel: Subnetting

Eine Organisation bekommt den Adressblock 131.42.0.0/16 zugewiesen und benötigt

- 1 Subnetz mit bis zu 32000 Hosts
- 15 Subnetze mit bis zu 2000 Hosts
- 8 Subnetze mit bis zu 250 Hosts

Machen Sie Vorschläge für eine Aufteilung in geeignete Subnetz-Adressen

Kapitel 2.3
DNS – Domain Name System

Namen im Internet

Einordnung

- IPv4-Adressen für (menschliche) Endnutzer „*ungünstig*“
- IP-Adressen sind (wegen hierarchischem Routing) an die Netztopologie gebunden. Wenn ein Host (oder Inhalt) also von einer Stelle im Internet an eine andere verlegt wird, ändert sich (in der Regel) die IP-Adresse.
- Gesucht: ein System um Hosts Namen zu geben, und diese Namen auf IP-Adressen abzubilden.

  ➔DNS (Domain Name System)
- Andere Ansätze: Aliasing, X.500, LDAP

Rahmenbedingungen

- In LAN einer einzigen Organisation wäre es möglich eine zentrale Liste von Hostnamen mit zugehörigen IP-Adressen zu führen
- Im Internet widerspricht ein zentralverwalteter Ansatz der Grundidee (und ist technisch problematisch)

https://ftp.isc.org/www/survey/reports/current/

- `Jan 2017|1,062,660,523`

(Hosts im DNS + zahlreiche unabhängige Akteure)

Herausforderungen bei der Namensvergabe

- Unabhängigkeit der Akteure
  - Kein globaler einheitlicher Zustand
  - Umziehen eines einzelnen Hosts muss allen mitgeteilt werden
- Skalierbarkeit
  - Abbildung von Namen auf Adressen muss für alle 2^{32} IPv4-Adressen bzw. 2^{64} IPv6-Adressen skalieren
  - Portierbarkeit auf nachfolgende größere Adressräume

Lösungsansätze

- Viele unabhängige Akteure:
  DNS-Namensraum als Baumstruktur ➔
  hierarchischer Namensraum
  - Einzelne Äste/Bereiche des Baums werden einzelnen Akteuren zugesprochen.
- Skalierbarkeit (große und wachsende absolute Zahl an Teilnehmern):
  Implementierung als verteilte Datenbank.
  - Bei Wachstum des Systems (bzw. Last) können einfach weitere DNS Server hinzugefügt werden.

Überblick DNS

DNS …

- ist ein Dienst der Anwendungsschicht
- ist als verteilte Datenbank mit einer Hierarchie von Nameservern implementiert.
- bietet einen als Baum strukturierten (hierarchischen) Namensraum für Hosts im Internet.
- ist kritischer Bestandteil des Internets!

DNS als Dienst

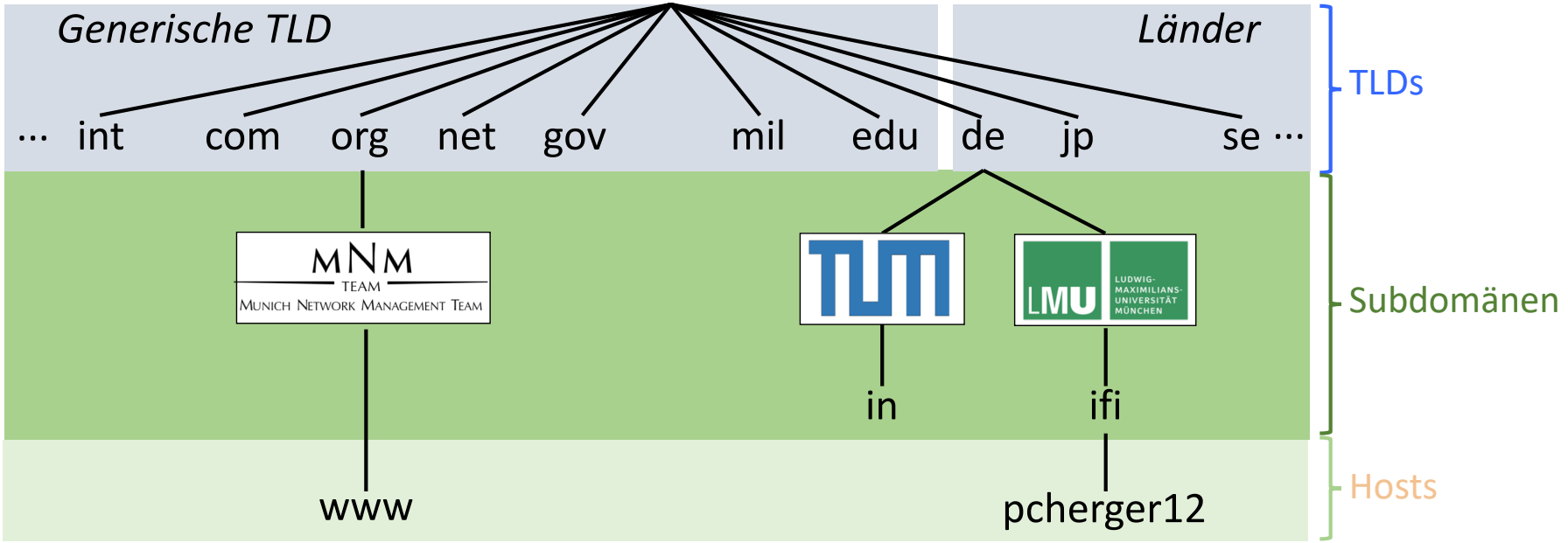
- Dienste und Dienstmerkmale:
  - Namensauflösung (Abbildung Host-Namen auf IP-Adressen
    - *Fully Qualified Domain-Name (FQDN)*
    - *Resource Records = <name> [<ttl>] [<class>] <type> <rdata>*
  - Aliasing (insbesondere für Hosts, Mail Server)
  - Redundanz
  - Lastverteilung zwischen replizierten Servern
- Grundfunktionen eines DNS-Servers:
  - Beantworten von Client-Anfragen
  - Austausch mit anderen DNS-Servern

Der DNS Namensraum (1)

- Unterscheidung: Generische und Länder-Domänen
- Top Level Domains (TLD) von der ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet
- Für jeden TLD gibt es einen Registrar, der (gegen Gebühr) second level Domains in diesem TLD an verschiedenste Organisationen (z.B.: LMU) sowie Privatleute vergibt (➔ First Come, First Served)

Der DNS Namensraum (2)

- Second Level Domains (und tiefer) können von den Organisationen, denen sie zugesprochen wurden, beliebig in weitere Subdomänen eingeteilt werden. (z.B.: „ifi“ als Subdomäne von „lmu“)
- Blätter des Baums enthalten Hostnamen (In der Praxis kann „Hostname“ mit vielen IP-Adressen /tatsächlichen Hostmaschinen assoziiert werden)
- Der *Fully Qualified Domain Name* (FQDN) ist der volle Pfad von einem Blatt des Baums bis zur Wurzel (durch Punkte getrennt) z.B.: „pcheger12.nm.ifi.lmu.de.“ (Die Wurzel nach dem letztem Punkt ist namenslos)



- Hierarchisch, Baumstruktur
- Top Level Domains (TLD): festgelegt von ICANN
  - generisch, nach Zweck (gTLD)
  - TLD für Länder (ccTLD, ca 240 Stück)
  - seit 2013: „new gTLDs“
- Subdomains: Unterteilung in benannte Teildomänen
  - Second-level domains (z.B. `lmu.de`) von Registraren zugeteilt
  - Unterteilung in Subdomains kann wiederholt werden
- Host-Name: Blätter des Baumes
- Fully Qualified Domain Name (FQDN)
  - vollständiger Name bestehend aus Hostname und Domänennamen
  - in Richtung Baumwurzel zu lesen; endet mit Punkt

Cybersquatting

- Engl. Squatter = Hausbesetzer
  - Domänenbesetzung, Domainsquatting, Namejacking, Brandjacking
- Registrierung von Domain-Namen, die für andere Personen oder Institutionen von Interesse sind
  - Markennamen, Musiker, Sportler, ...
- Verkauf der Namen
- Rechtliche Situation

Ressourcendatensätze (Engl.: Resource Records)

- Die durch DNS implementierte Datenbank enthält als Daten sogenannte Resource Records (RR)
- Jede Domäne kann mit beliebiger Anzahl von RRs assoziiert sein
- Resource Records sind (zur Effizienz) binär codierter Fünftupel mit folgendem Schema: (<Domain Name>,<TTL>,<Klasse>,<Typ>,<Wert>)

Resource Records

- *Resource Records* sind ein (zur Effizienz) binär codierter Fünftupel mit folgendem Schema:
  (<Domain Name>,<TTL>,<Klasse>,<Typ>,<Wert>)
  - Der **Domain Name** ist normalerweise der primäre Suchschlüssel für die Anforderung von RRs (z.B.: „lmu.de“).
  - **TTL** (engl.: time to live) ist die Zeit in Sekunden für die, die Instanz des RR als gesichert (wahrscheinlich korrekt) gilt.
  - Das **Klasse** Feld enthält in der Praxis fast immer den wert „IN“ für „Internet“.
  - Eine Auswahl von RR **Typen** gibt es auf der nächsten Folie.
  - Der **Wert** sind die eigentlichen Daten des RRs.

Wichtige RR Typen

Typ	Bedeutung	Zugehöriger Wert
SOA	Start of Authority	Infos zur Zonen Verwaltung
A	IPv4 Address Record	32-bit Integer, IPv4-Adresse
AAAA	IPv6 Address Record	128-bit Integer, IPv6-Adresse
MX	Mail Exchange Record	Zuordnung der zuständigen Mailserver
NS	Nameserver Record	Hostname eines autoritativen Nameservers
CNAME	Canonical Name Record	Kanonischer Name eines Hosts
PTR	Pointer	Für Reverse Mapping: IP-Adressen➔Namen
TXT	Text Record	Ursprünglich frei definiert, heute SPF (Sender Policy Framework), DomainKeys, DMARC, DNS-SD, Google-Site Verificiation

Zonen im DNS Namensraum

- DNS Namensraum wird in **nicht überlappende administrative Zonen** aufgeteilt
- Administratoren einer Zone stellen für Anfragen zu beliebigen FQDNs in ihrer Zone „**autoritative Nameserver**“ bereit

- Anmerkung: Die Administratoren einer Zone sind nicht unbedingt identisch mit den Inhabern der zugehörigen Domänen

Autoritative Nameserver

- Antworten von „*autoritativen Nameserver*“ gelten als richtig
- Allgemein: zur **Lastverteilung/Ausfallsicherheit mehrere autoritative Nameserver** pro Zone bereitgestellt
  - Ein primärer Nameserver (wird aktiv gewartet)
  - Alle anderen sind sekundäre Nameserver (holen regelmäßig aktuelle Informationen vom primären Nameserver per „Zonentransfer“)
  - Primäre und sekundäre Nameserver einer Zone gelten gleichermaßen als autoritativ.

Weitere Nameserver-Typen

- Root Nameserver
  - 13 Root-Nameserver weltweit
  - gut geschützte stark replizierte Hochleistungssysteme (werden per *anycast routing* angesteuert)
  - kennen vor allem die autoritativen Nameserver der top-level Domänen (sowie die populärer second-level Domänen)
- Lokale Nameserver
  - Hosts im Internet müssen mindestens einen Nameserver mit IP-Adresse kennen, um überhaupt eine Anlaufstelle für die Namensauflösung (und damit das Ermitteln weiterer IP-Adressen) zu haben ➔ Lokaler Nameserver des Hosts
  - Werden vor allem von ISPs bereitgestellt.

Anfragen an DNS - Ablauf

1. **Anfrage** an Resolver (lokales Programm des Hosts)
2. Nachschlagen im Cache – Ergebnis? (Ja / Nein)

Nein

3. **Anfrage** an lokalen Nameserver
4. Nachschlagen im Cache – Ergebnis? (Ja / Nein)

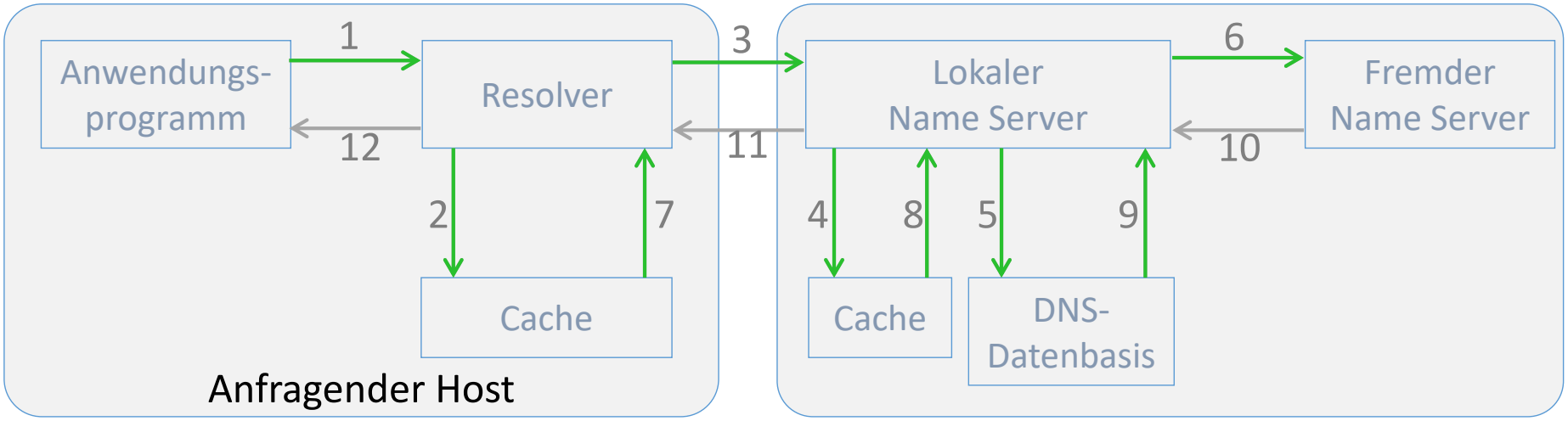
Nein

5. Nachschlagen in RRs des lokalen NS – Ergebnis? (Ja / Nein)

Nein

6. **Anfrage** an fremde Nameserver – Ergebnis?

Achtung: RRs in einem Cache sind niemals autoritativ und werden nach Ablauf der *time-to-live* (TTL) verworfen!



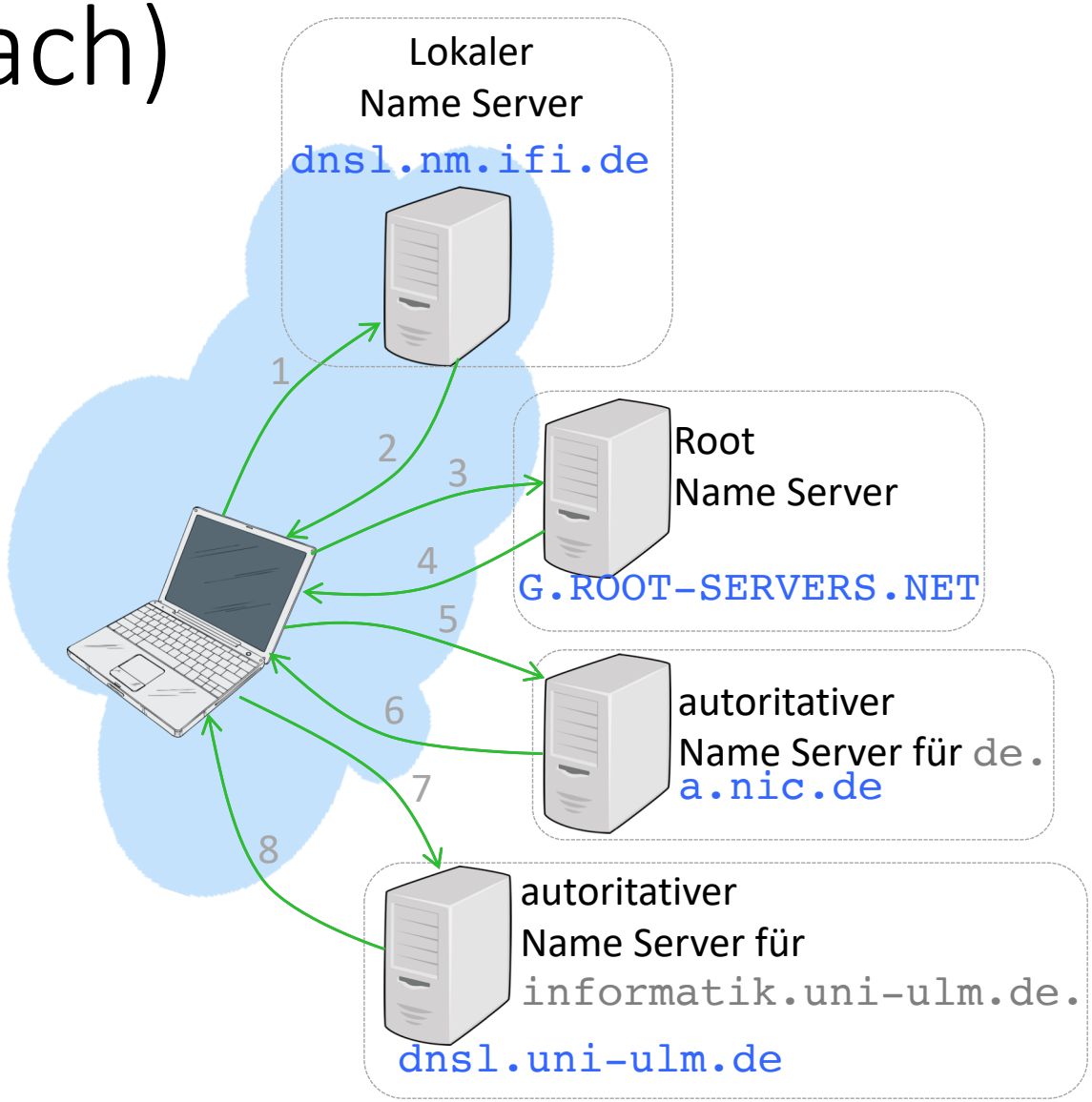
- Schritte
  1. Anfrage an den Resolver (lokal auf Host)
  2. Nachschlagen im Cache.(Bei Erfolg: 7, 12)
  3. Anfragen bei lokalem DNS-Server
  4. Nachschlagen in Datenbasis.(Bei Erfolg: 9, 11, 12)
  5. Nachschalgen im Cache.
  6. Anfrage an fremden DNS-Server. Antwort: 10, 11, 12
     (Bei Erfolg: 8, 11, 12 + Update Resolver-Cache)
- Inhalt der Antwort
  - gesuchte IP-Adresse, oder
  - Referenz auf DNS-Server, der den Name auflösen kann, oder
  - „gibt es nicht“
- Antwort führt zur Auffrischung der Cache-Information

Abarbeitung der DNS Anfragen

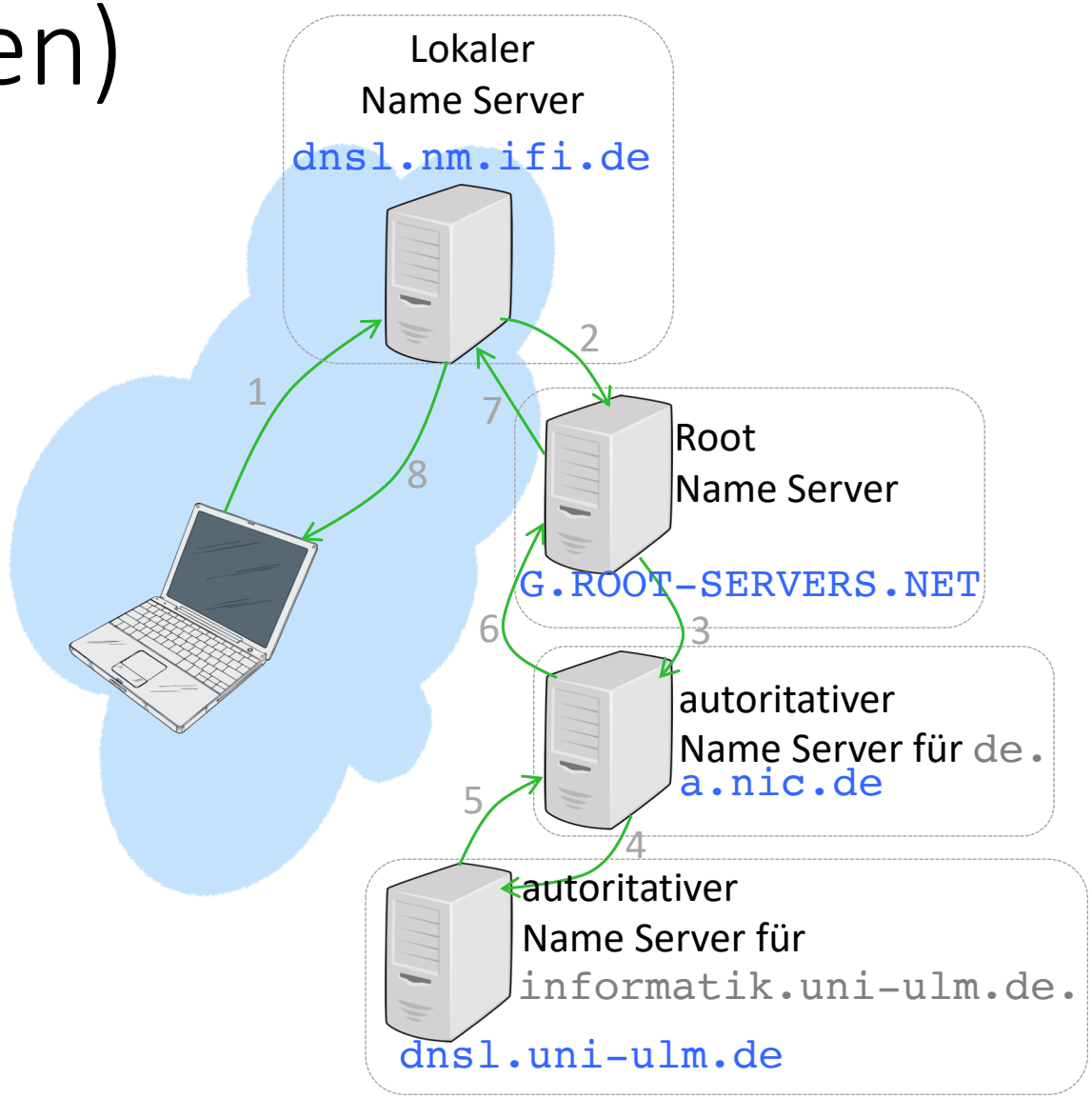
- Man unterscheidet
  - Iterative Anfragen
  - Rekursive Anfragen

- Iterative Anfragen geben jeweils Teilantwort der Anfrage (z.B.: Root Nameserver gibt nur den NS für „.de“ als Antwort zur Anfrage „dns1.nm.ifi.lmu.de“)
- Rekursive Anfragen geben immer vollständige Antwort, erhöhen aber die Last auf beteiligte Nameserver (außerdem Sicherheitsrisiken)

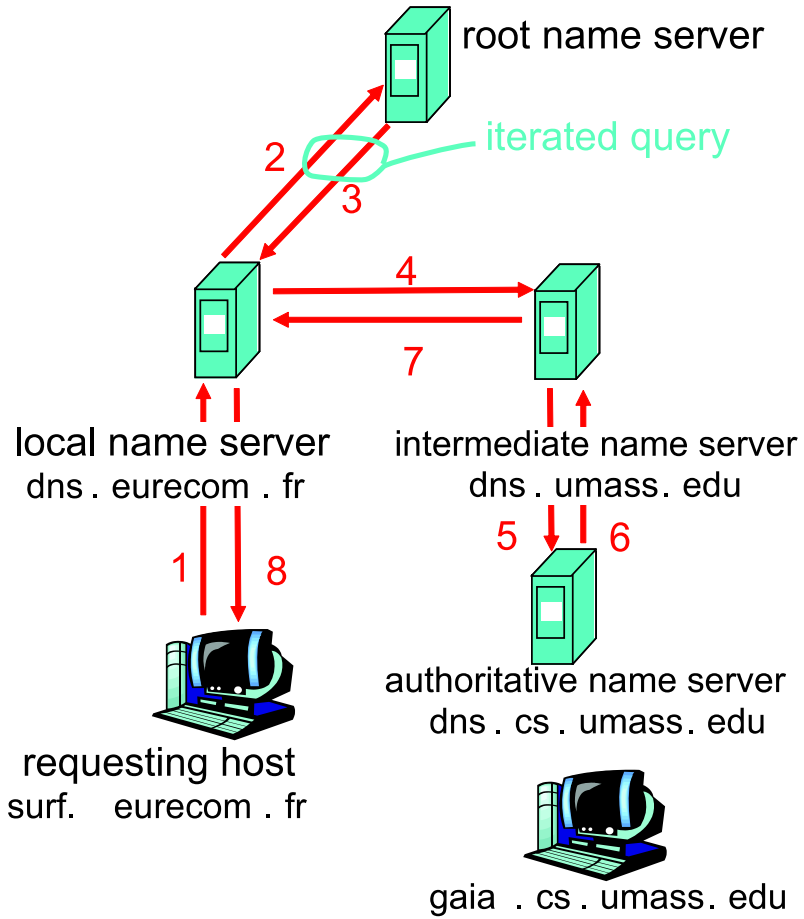
DNS: Iterative Anfrage (Der Reihe nach)



DNS: Rekursive Anfrage: (Durchreichen)



Regelfall: kombinierter Ansatz



- In der Praxis meist Kombination aus rekursiven/iterativen Anfragen. (Sofern die gewünschte Information nicht schon in einem Cache vorhanden ist)
- Root Nameserver beantworten Anfragen im allgemeinen nicht rekursiv.
- Hosts stellen allgemein rekursive Anfragen an ihren lokalen Nameserver. Dieser arbeitet sie iterativ ab.

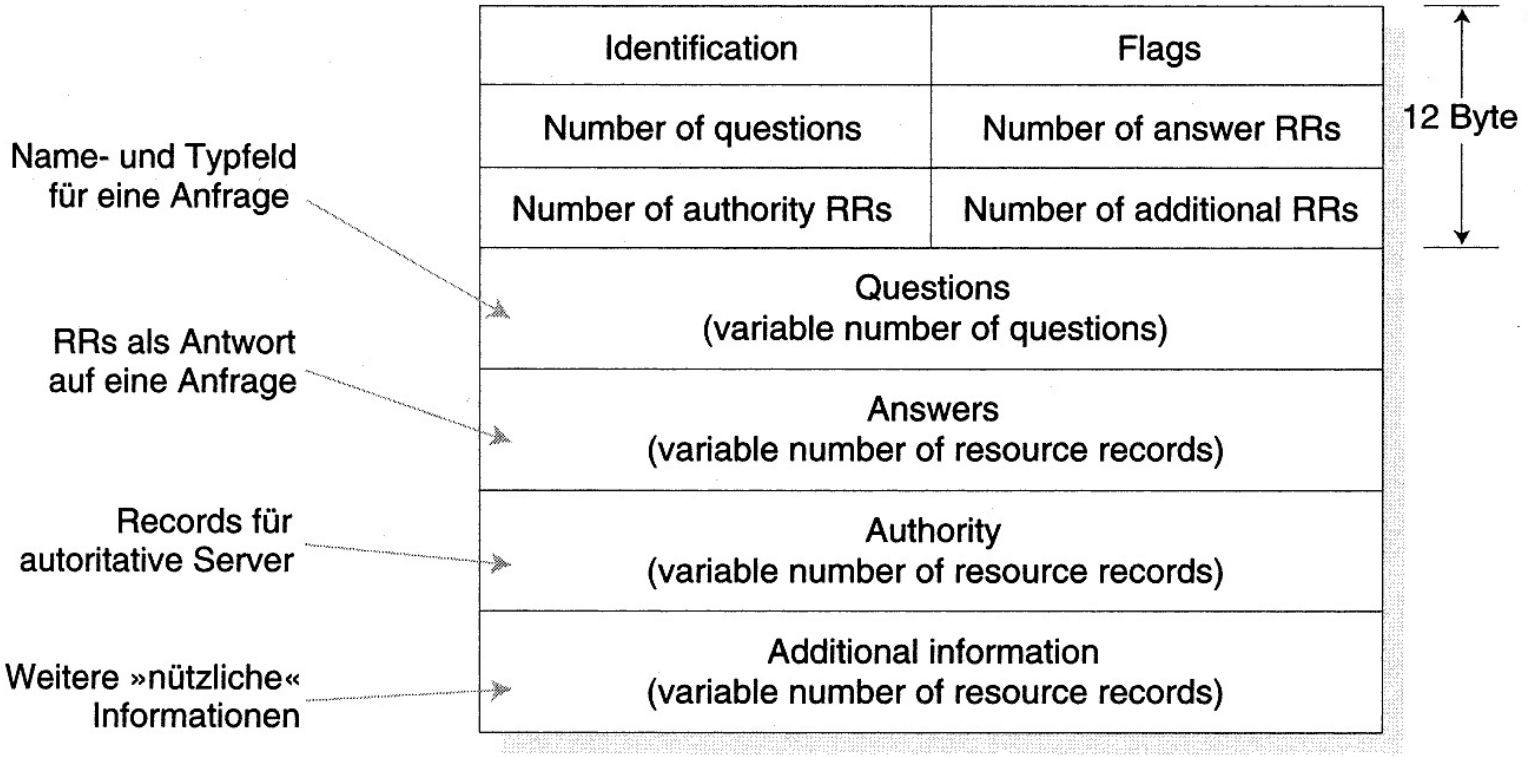
Beispielanfrage: host und dig

```
danciu@pcheger09:~> host www.in.tum.de
www.in.tum.de is an alias for www.informatik.tu-muenchen.de.
www.informatik.tu-muenchen.de is an alias for infoport.informatik.tu-muenchen.de.
infoport.informatik.tu-muenchen.de has address 131.159.74.65
infoport.informatik.tu-muenchen.de mail is handled by 25 mailin.informatik.tu-muenchen.de.
```

```
; <<>> DiG 9.3.4 <<>> www.in.tum.de
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7702
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 7
;; QUESTION SECTION:
;www.in.tum.de.                 IN      A
;; ANSWER SECTION:
www.in.tum.de.          86400   IN      CNAME   www.informatik.tu-muenchen.de.
www.informatik.tu-muenchen.de. 86400 IN CNAME   infoport.informatik.tu-muenchen.de.
infoport.informatik.tu-muenchen.de.     86400   IN      A       131.159.74.65
[...]
```

Name, TTL, Class, Type, Value

DNS-PDU Format



- Identification: Anfrage ID
- Flags: Query/Reply, Authoritative Bit, Recursion Desired, Recursion Available

Wahl des Transportprotokolls

- Anfragen: UDP-basiert (Performanz)
  - Verzicht auf Verbindungsaufbau
  - Anfragen zustandslos
  - Wiederholung möglich, falls Frage oder Antwort verloren gehen
- Zonentransfer: TCP-basiert (Zuverlässigkeit)
  - Größeres Datenvolumen als einzelne Anfrage
  - Findet im Vergleich zu Anfragen selten statt

- Details zu TCP/UDP ➔ Kapitel 3

Fragen zu Kapitel 2 (1/2)

- Welche Maßnahmen zur Begegnung von IPv4 Adressknappheit wurden in der Vorlesung behandelt?
- Wie viele Hosts kann ein IPv4 Adressblock mit einer Präfixlänge von 22 maximal fassen?
- In welches der folgenden Subnetze des Netzes 184.212.0.0/16 gehört die Adresse 184.212.2.36?
  - 184.212.128.0/17
  - 184.212.0.0/18
  - 184.212.96.0/19

Fragen zu Kapitel 2 (2/2)

- Wie unterscheiden sich die Rollen eines lokalen und eines autoritativen Nameservers? Kann ein einziger Server beide gleichzeitig erfüllen?
- Was sind die Unterschiede zwischen einer DNS Domäne und einer DNS Zone?