Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dipl.-Ing. Stephan Günther, M.Sc.
Johannes Naab, M.Sc.

Tutorübung zur Vorlesung Grundlagen Rechnernetze und Verteilte Systeme

Übungsblatt 11 (6. Juli – 10. Juli 2015)

Hinweis: Die mit * gekennzeichneten Teilaufgaben sind ohne Kenntnis der Ergebnisse vorhergehender Teilaufgaben lösbar.

Aufgabe 1 Domain Name System (DNS)

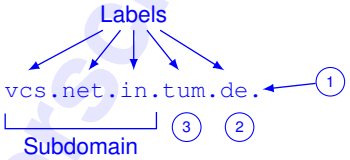
Zentrale Aufgabe des Domain Name Systems (DNS) ist es, menschenlesbare Namen auf IP-Adressen abzubilden, die dann für die Wegwahl auf der Netzwerkschicht verwendet werden können. Bei dem für die Vorlesungsunterlagen bekannten Namen `vcs.net.in.tum.de.` handelt es sich um einen sog. *Fully Qualified Domain Name (FQDN)*.

a)* Was ist der Unterschied zwischen einem vollqualifizierten Domain Name (FQDN) und einem nicht-(voll)qualifizierten?

Ein FQDN endet stets mit `.`, d. h. der Wurzel des Name Spaces. Ein nicht-qualifizierter Domain Name hingegen kann ein einzelnes Label oder eine Menge durch Punkte getrennte Labels sein, die relativ zu einer anderen Wurzel als `.` zu sehen sind.

b)* Benennen Sie die einzelnen Bestandteile des FQDNs, sofern es dafür gängige Bezeichnungen gibt.

1. Root (Beginn des Namensraums)
2. Top Level Domain (TLD)
3. Second Level Domain



Da im Alltag zumeist nicht explizit zwischen einem „FQDN“ (also mit terminierenden Punkt) und „Domain Name“ (also ohne terminierenden Punkt) unterschieden wird, da es kontextabhängig klar ist, was von beiden gerade gemeint ist, werden wir[1] im Folgenden auch nur noch dann den Root-Punkt setzen, wenn wir dies besonders hervorhaben bzw. deutlich machen wollen.

In Abbildung 1 sind ein PC sowie eine Reihe von Servern dargestellt. Wir nehmen an, PC1 nutze einen Resolver von Google unter der IP-Adresse 8.8.8.8 zur Namensauflösung. Ferner nehmen wir an, dass der Google-Resolver gerade neu gestartet wurde (also insbesondere keine Resource Records gecached hat) und rekursive Namensauflösung anbietet. Der Server `D.ROOT-SERVERS.NET` sei ein Root-Nameserver während `F.NIC.de` einer der autoritativen Namensserver für `de`-TLDs ist.

c)* Erläutern Sie den Unterschied zwischen einem *Resolver* und einem *Nameserver*.

Nameserver sind autoritativ für eine oder mehrere Zonen („Bereiche“), d. h. sie besitzen eine gültige und aktuelle Kopie der gesamten Zone, für die sie autoritativ sind.
Resolver hingegen extrahieren mittels eine Reihe iterativer Anfragen an die jeweils autoritativen Nameserver die benötigten Information aus dem DNS und geben diese an den anfragenden Client zurück. Resolver können Einträge für begrenzte Zeit cachen, so dass bei erneuter Anfrage desselben Resource Records der Prozess nicht wiederholt werden muss.

d)* Welche Funktion erfüllen `D.ROOT-SERVERS.NET` und `F.NIC.de`?

Der Root-Nameserver ist autoritativ für die Rootzone, d. h. er kennt die Nameserver, welche für die einzelnen TLDs verantwortlich sind, so z. B. `F.NIC.de` als einen der autoritativen Namensserver für de-Domains.
`F.NIC.de` kennt wiederum die zuständigen Namensserver für alle Second-Level-Domains unterhalb der de-TLD.

e)* Für welche Zonen sind die Server `ns.tum.de`, `ns.in.tum.de` und `ns.net.in.tum.de` (vermutlich) autoritativ?

Die FQDNs der Server lassen vermuten, dass sie jeweils für `tum.de`, `in.tum.de` und `net.in.tum.de` verantwortlich sind. Allerdings sollte man nicht aus dem FQDN eines Nameservers voreilige Schlüsse über ziehen: der FQDN eines Servers ist i. A. unabhängig von den Zonen, für die er autoritativ ist.

f) Zeichnen Sie in Abbildung 1 alle DNS-Nachrichten (Request / Response) ein, die ausgetauscht werden, sobald PC1 auf `vcs.net.in.tum.de.` zugreift. Nummerieren Sie die Nachrichten gemäß der Reihenfolge, in der sie zwischen den einzelnen Knoten ausgetauscht werden.

[1] for the sake of notational brevity

s. Abbildung 1.

g) Erklären Sie den Unterschied zwischen iterativer und rekursiver Namensauflösung.

Rekursive Namensauflösung bedeutet, dass eine DNS-Anfrage an einen Resolver gestellt wird. Dieser wird das endgültige Ergebnis zurücksenden.
Bei iterativer Auflösung hingegen werden schrittweise die autoritativen Namensserver der einzelnen Zonen angefragt.

h)* Wie wird im DNS sichergestellt, dass kein bösartiger Nameserver Anfragen für andere Domänen beantwortet? (Wir gehen davon aus, dass keine Man-in-the-Middle-Angriffe möglich sind.)

Dies wird lediglich indirekt dadurch sichergestellt, dass während der iterativen Namensauflösung stets nur die jeweils autoritativen Namensserver kontaktiert werden. Sofern die

- Antwort des Rootservers zuverlässig war und
- die Antwort auf dem Weg vom Rootserver zum anfragenden Namensserver nicht modifiziert wurde

kann ein bösartiger Namensserver keine falschen Antworten liefern – eben da er nie gefragt wird.
Selbstverständlich wird auf diese Weise nicht verhindert, dass DNS-Antworten mittels Man-in-the-Middle-Attacken abgefangen und modifiziert werden können. Dagegen helfen lediglich kryptographische Verfahren, wie sie in der DNSSEC-Erweiterung zu finden sind (nicht in der Vorlesung behandelt).

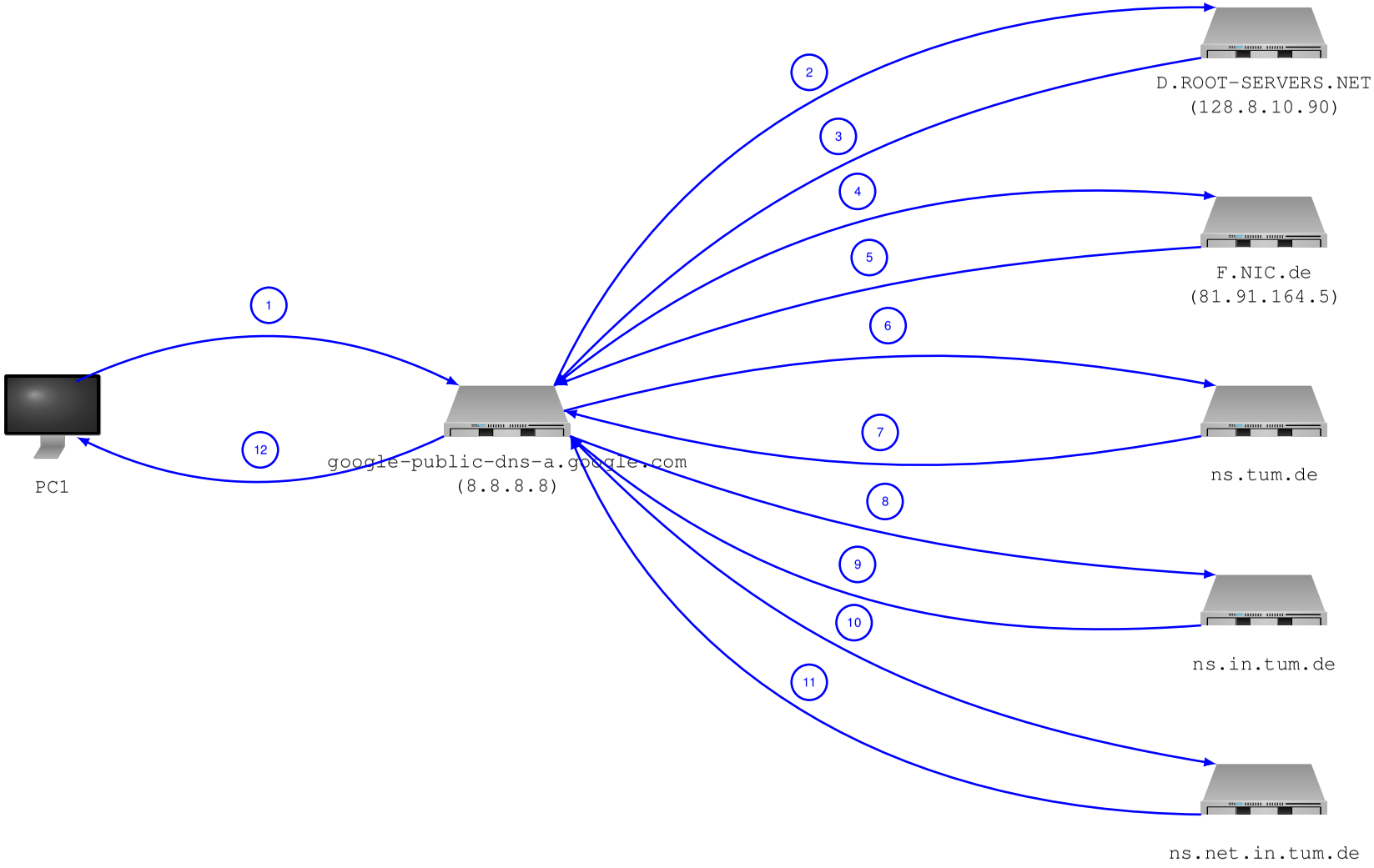


Abbildung 1: Loesungsblatt zu Aufgabe.

Aufgabe 2 DNS nochmal

Gegeben Sie die folgende Menge von Domain Names:

- `tum.de.`
- `www.tum.de.`
- `in.tum.de.`
- `ei.tum.de.`
- `mw.tum.de.`
- `www.in.tum.de.`
- `www.ei.tum.de.`
- `www.mw.tum.de.`
- `net.in.tum.de.`
- `www.net.in.tum.de.`
- `vcs.net.in.tum.de.`
- `phobia.net.in.tum.de.`
- `paranoia.net.in.tum.de.`
- `svm000.net.in.tum.de.`
- `svm001.net.in.tum.de.`
- `google-public-dns-a.google.com.`

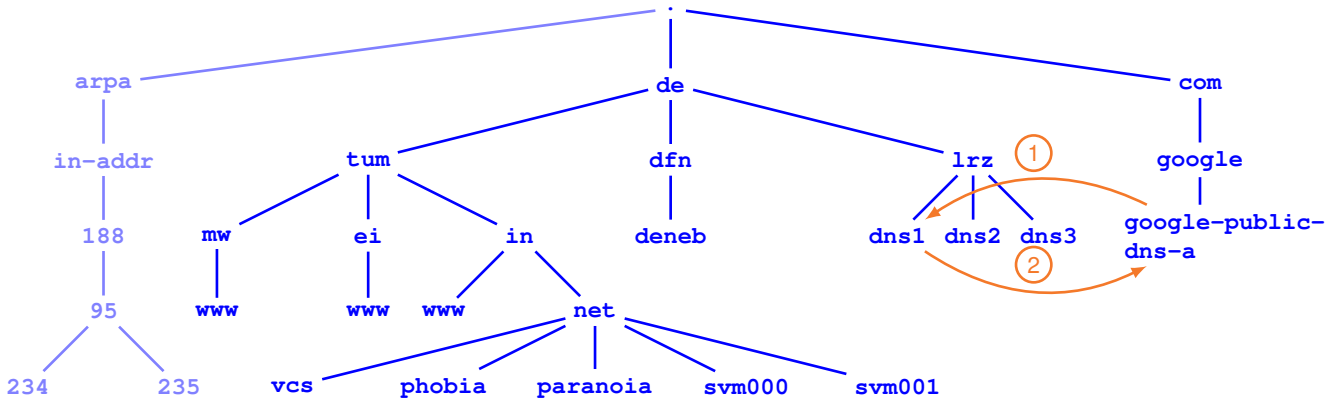
Name Server:

- `dns1.lrz.de.`
- `dns2.lrz.de.`
- `dns3.lrz.de.`
- `deneb.dfn.de.`

Abbildung 2: Einige FQDNs der TUM.

a)* Stellen Sie basierend auf den gegebenen Domain Names (einschließlich die der Nameserver) den Name Space als Baum beginnend bei der Wurzel `.` dar.

Die orange Lösung gehört zu Teilaufgabe c). Die hellblaue Lösung gehört zu Teilaufgabe e).



b)* Stellen Sie mittels des Kommandozeilenprogramms `dig` (Linux / OS X) bzw. `nslookup` (Windows) fest, welche der in Abbildung 2 aufgelisteten Nameserver jeweils für die Zonen `tum.de`, `in.tum.de`, `ei.tum.de`, `mw.tum.de` und `net.in.tum.de` autoritativ sind.

Wichtig: Leider unterscheiden sich die Antworten, wenn sie beispielsweise aus Eduroam gestellt werden (was sie eigentlich nicht sollten). Es ist möglich, dass dies auch aus anderen Teilen Des Universitätsnetzes geschieht. Grund scheint ein interessantes Setup der Rechnerbertriebsgruppe zu sein.
Damit Sie reproduzierbare Antworten erhalten, nutzen Sie am besten einen der Google-Resolver: **`dig tum.de NS @8.8.8.8`**

`dig tum.de NS` ergibt beispielsweise:

```
moepi@mjolnir tutorial11 % dig tum.de NS

; <<>> DiG 9.9.5-9-Debian <<>> tum.de NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36141
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tum.de. IN NS

;; ANSWER SECTION:
```

```
tum.de. 86400 IN NS dns3.lrz.eu.
tum.de. 86400 IN NS dns1.lrz.de.
tum.de. 86400 IN NS dns2.lrz.bayern.

;; Query time: 2 msec
;; SERVER: 10.211.55.1#53(10.211.55.1)
;; WHEN: Thu Jul 02 12:47:28 CEST 2015
;; MSG SIZE  rcvd: 112
```

Der Answer Section ist zu entnehmen, dass von den gegebenen Name Servern lediglich `dns1.lrz.de.` autoritativ ist. Die anderen beiden Name Server sind (damits nicht so viel zu schreiben wird) nicht Teil der Aufgabenstellung.
Weitere Anfragen ergeben:

	`dns1.lrz.de.`	`dns2.lrz.de.`	`dns3.lrz.de.`	`deneb.dfn.de.`
`tum.de.`	x			
`in.tum.de.`	x	x	x	x
`ei.tum.de.`	x			
`mw.tum.de.`	x	x	x	
`net.in.tum.de.`	x	x	x	

c) Zeichnen Sie in den Namespace die Abfolge der DNS-Nachrichten ein, die entsteht, wenn der Resolver `google-public-dns-a.google.com` versucht, den FQDN `vcs.net.in.tum.de.` aufzuösen. Gehen Sie davon aus, dass dem Resolver aus vorherigen Anfragen bereits `dns1.lrz.de.` als autoritativer Nameserver für `tum.de.` bekannt ist.

siehe Lösung von Teilaufgabe a):

- Im ersten Schritt wird sich der Resolver sicher an `dns1.lrz.de.` wenden, da er laut Angabe der einzige autoritative Name Server für `tum.de.` ist.
- Da `dns1.lrz.de.` sowohl für `tum.de.` als auch für `net.in.tum.de.` autoritativ ist, wird keine Delegation an weitere Name Server mehr stattfinden.
- Stattdessen erhält der Resolver in diesem Fall bereits von `dns1.lrz.de.` den A Record für `vcs.net.in.tum.de.`.

Die in der Vorlesung bzw. den Programmieraufgaben verwendeten virtuellen Maschinen haben Adressen aus dem Subnetz 188.95.234.0/23.

d)* Erläutern Sie, wie der IPv4-Adressbereich in den DNS Namespace eingebettet wird.

IPv4-Adressen werden oktett-weise in umgekehrter Reihenfolge als Labels interpretiert und unterhalb des FQDNs `in-addr.arpa.` gespeichert.

e) Ergänzen Sie Ihre Lösung von Teilaufgabe a) um die FQDNs der zugehörigen Reverse Lookup Zones.

s. Lösung von Teilaufgabe 1).

f)* Stellen Sie fest, welche Nameserver autoritativ für die Reverse Lookup Zones dieses Adressbereichs sind.

`dig 234.95.188.in-addr.arpa. NS` und `dig 235.95.188.in-addr.arpa.` ergeben, dass die beiden Nameserver `lucifer.net.in.tum.de.` und `nimbus.net.in.tum.de.` autoritativ sind.

g)* Aus welchem Grund ist es im DNS nicht möglich, die beiden Subnetze 188.195.234.0/24 und 188.195.235.0/24 mit nur einer Zone abzubilden?

Die beiden Netze lassen sich zwar im IP-Adressraum zum Netz 188.195.234.0/23 zusammenfassen, allerdings ist das nicht auf den DNS Name Space übertragbar, da hier keine Subnetzmasken oder Präfixlängen gespeichert werden. Der DNS Namespace orientiert sich vielmehr an den Adressklassen.
Die einzige Möglichkeit `235.95.188.in-addr.arpa.` weiter zu deligieren besteht darin, eine eigene Zone für jede einzelne Adresse innheralb des /24 Subnetzes zu erzeugen – Aufwand.

Hinweis: RFC 2317 beschreibt eine Möglichkeit, diese Beschränkung zu umgehen. Diese ist jedoch auch nicht „einfacher“, als einfach eine Zone pro Adresse zu erzeugen...