Lehrstuhl für Netzarchitekturen und Netzdienste
School of Computation, Information and Technology
Technische Universität München

Grundlagen Rechnernetze und Verteilte Systeme (IN0010)

Übungsblatt 12

13. Juli – 17. Juli 2026

Aufgabe 1 Domain Name System (DNS)

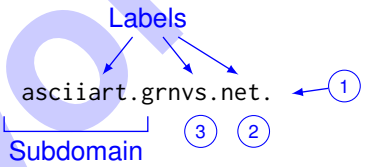
Zentrale Aufgabe des Domain Name Systems (DNS) ist es, menschenlesbare Namen auf IP-Adressen abzubilden, die dann für die Wegwahl auf der Netzwerkschicht verwendet werden können. Bei dem Namen `asciiart.grnvs.net.` handelt es sich um einen sog. *Fully Qualified Domain Name (FQDN)*.

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 geordnete Liste durch Punkte getrennter 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 im Folgenden auch nur noch dann den Root-Punkt setzen, wenn wir dies besonders hervorheben bzw. deutlich machen wollen.

In Abbildung 1.1 sind ein PC sowie eine Reihe von Servern dargestellt. Wir nehmen an, dass PC1 den Router als Resolver nutzt. Der Router wiederrum nutzt 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.
Die autoritativen Nameserver für die jeweiligen Zonen sind in Tabelle 1.1 gegeben.

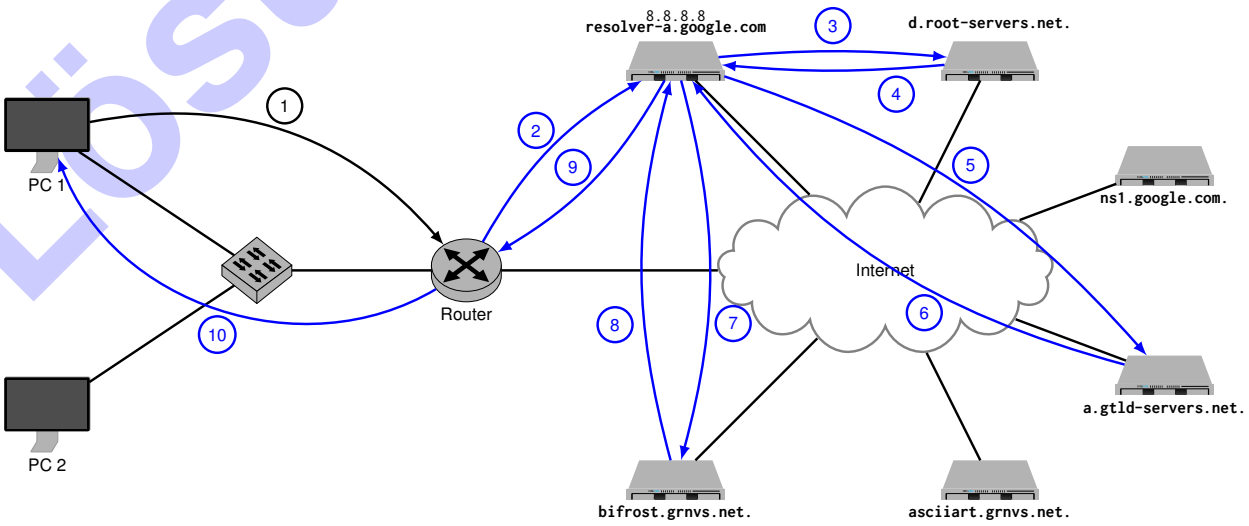


Abbildung 1.1: Vorlage zu Aufgabe 1f)

Zone	autoritativer Nameserver
.	d.root-servers.net.
com., net.	a.gtld-servers.net.
google.com.	ns1.google.com.
grnvs.net.	bifrost.grnvs.net.

Tabelle 1.1: Zonen mit zugehörigen autoritativen Nameservern

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 derselben Resource Records der Prozess nicht wiederholt werden muss.

d)* Welche Funktion erfüllen `d.root-servers.net` und `a.gtld-servers.net`?

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

e)* 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 Nameserver der einzelnen Zonen angefragt.

f) Zeichnen Sie in Abbildung 1.1 alle DNS-Nachrichten (Requests / Responses) ein, die ausgetauscht werden, sobald PC1 auf `asciiart.grnvs.net.` zugreift. Nummerieren Sie die Nachrichten gemäß der Reihenfolge, in der sie zwischen den einzelnen Knoten ausgetauscht werden.

g)* 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 Nameserver kontaktiert werden. Sofern die

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

kann ein bösartiger Nameserver 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).

Aufgabe 2 DNS Zonefile

Sie sind HiWi am Lehrstuhl und haben die Aufgabe bekommen eine Zonendatei für `grnvs.net.` zu erstellen. Relevante Server und deren Domainnamen und IP Adressen sind in Abbildung 2.1 zu sehen.
Füllen Sie die folgende Vorlage so aus, dass die Anforderungen der einzelnen Teilaufgaben erfüllt werden. Tragen Sie für die folgenden Teilaufgaben den Buchstaben der zugehörigen Teilaufgabe in die Box am Ende jeder Zeile ein.

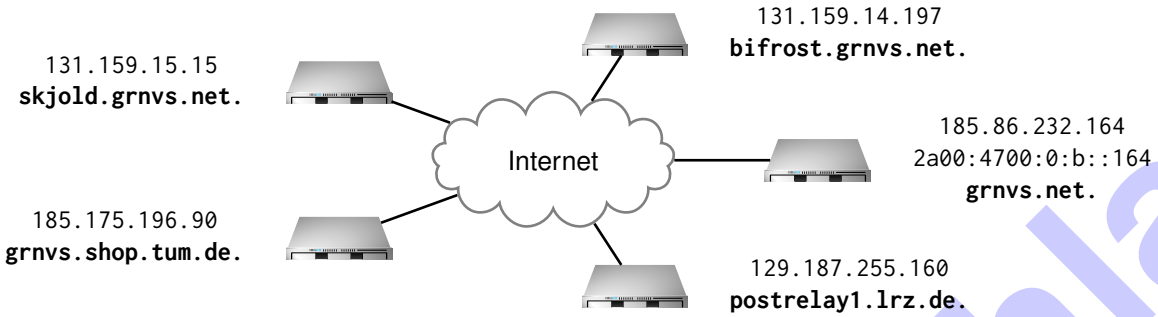


Abbildung 2.1: Für die Zone `grnvs.net.` relevante Server mit Domainnamen und IP Adressen

grnvs.net.	**600**	**IN**	**SOA**	**bifrost.grnvs.net. admin.grnvs.net. 1783475002 3600 900 604800 900**	
grnvs.net.			**NS**	**bifrost.grnvs.net.**	**a)**
grnvs.net.			**NS**	**skjold.grnvs.net.**	**a)**
bifrost.grnvs.net.			**A**	**131.159.14.197**	**b)**
skjold.grnvs.net.			**A**	**131.159.15.15**	**b)**
grnvs.net.			**A**	**185.86.232.164**	**c)**
grnvs.net.			**AAAA**	**2a00:4700:0:b::164**	**c)**
grnvs.net.			**MX**	**10 postrelay1.lrz.de.**	**d)**
shop.grnvs.net.			**CNAME**	**grnvs.shop.tum.de.**	**e)**

a)* Der primäre Nameserver der Zone ist `bifrost.grnvs.net` und bereits eingetragen. Zur Ausfallsicherheit soll der Server, der unter `skjold.grnvs.net` erreichbar ist, als sekundärer Nameserver agieren.

b)* Stellen Sie sicher, dass die Nameserver jeweils unter ihren IP Adressen erreichbar sind.

c)* Wenn man `grnvs.net` im Browser aufruft, soll die GRNVS Website angezeigt werden. Dies funktioniert aktuell nur für IPv4, sie soll auch über IPv6 erreichbar sein.

d)* Damit Studierende eine E-Mail an `info@grnvs.net` schicken können, muss ein Mailserver eingetragen werden. Um diesen nicht selbst betreiben zu müssen, soll mit Priorität 10 der LRZ E-Mail Service Postrelay verwendet werden.

e)* Im kommenden Semester sollen GRNVS Fanartikel und Bonuspunkte verkauft werden. Damit kein eigener Online Shop betrieben werden muss, wurde eine Kooperation mit dem TUM Shop vereinbart. Für den Zugriff soll `shop.grnvs.net` als Alias für `grnvs.shop.tum.de` dienen.

f)* Warum ist es hier nicht möglich `grnvs.net.cit.tum.de.` als Alias für `grnvs.net.` zu konfigurieren?

Die Domain `grnvs.net.cit.tum.de.` liegt in der Zone `net.cit.tum.de.` und nicht in `grnvs.net.`.

Aufgabe 3 DNS nochmal (Zusatzaufgabe)

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.`
- `git.net.in.tum.de.`
- `phobia.net.in.tum.de.`
- `paranoia.net.in.tum.de.`
- `svm0000.net.in.tum.de.`
- `svm0001.net.in.tum.de.`
- `google-public-dns-a.google.com.`

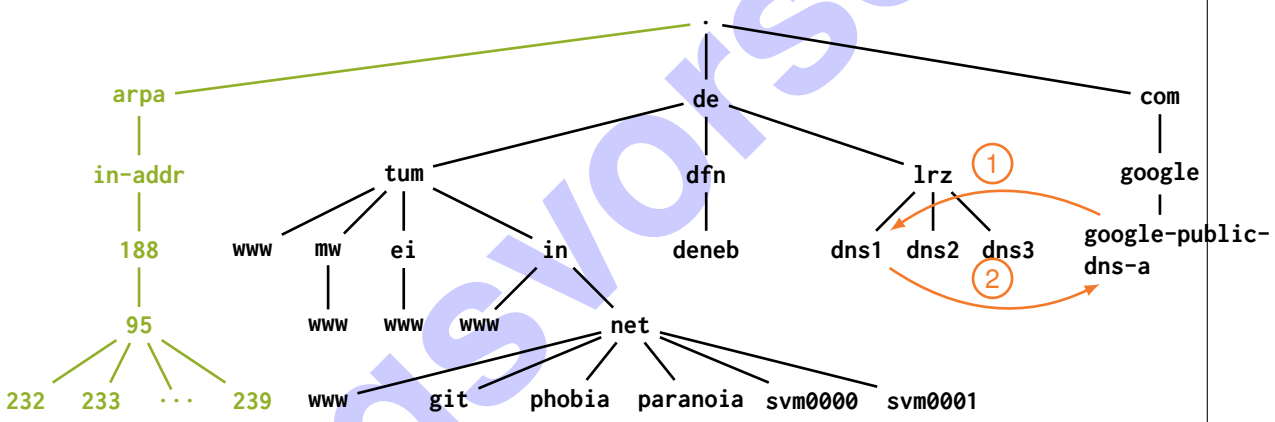
Nameserver:

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

Abbildung 3.1: Einige FQDNs.

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

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



b)* Stellen Sie mittels des Kommandozeilenprogramms `dig` (Linux / macOS) bzw. `nslookup` (Windows) fest, welche der in Abbildung 3.1 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 @8.8.8.8 tum.de NS`
`dig tum.de NS` ergibt beispielsweise:

```
root@svm0048:~# dig @8.8.8.8 NS tum.de

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> @8.8.8.8 NS tum.de
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 825
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;tum.de.                                IN      NS

;; ANSWER SECTION:
tum.de.                 12197   IN      NS      dns3.lrz.eu.
tum.de.                 12197   IN      NS      dns2.lrz.bayern.
tum.de.                 12197   IN      NS      dns1.lrz.de.

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jul 03 14:46:12 CEST 2016
;; MSG SIZE  rcvd: 112
```

Der Answer Section ist zu entnehmen, dass von den gegebenen Nameservern lediglich `dns1.lrz.de.` autoritativ ist. Die anderen beiden Nameserver sind (zur Minderung des Schreibaufwands) 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
ei.tum.de.	x			
mw.tum.de.	x	x	x	
net.in.tum.de.	x			

c) Zeichnen Sie in den Namespace (Lösung von Teilaufgabe a)) die Abfolge der DNS-Nachrichten ein, die entsteht, wenn der Resolver `google-public-dns-a.google.com` versucht, den FQDN `git.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 Nameserver 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 Nameserver mehr stattfinden.
- Stattdessen erhält der Resolver in diesem Fall bereits von `dns1.lrz.de.` den A Record für `git.net.in.tum.de.`.

Die in der Vorlesung bzw. den Programmieraufgaben verwendeten virtuellen Maschinen haben Adressen aus dem Subnetz 188.95.232.0/21.

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.

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

```
# dig +noall +answer 232.95.188.in-addr.arpa. NS
232.95.188.in-addr.arpa. 258    IN      NS      nimbus.net.in.tum.de.
232.95.188.in-addr.arpa. 258    IN      NS      lucifer.net.in.tum.de.
232.95.188.in-addr.arpa. 258    IN      NS      dns2.net.in.tum.de.
232.95.188.in-addr.arpa. 258    IN      NS      dns3.net.in.tum.de.
```

Die Outputs sollten zeigen, dass vier autoritative Nameserver existieren. Löst man deren IP-Adressen auf, stellt man fest, dass es lediglich zwei DNS-Server sind: `lucifer.net.in.tum.de.` und `nimbus.net.in.tum.de.`.

g)* Aus welchem Grund ist es im DNS nicht möglich, die 4 Subnetze 188.95.232.0/24, 188.95.233.0/24, 188.95.234.0/24 und 188.95.235.0/24 mit nur einer Reverse Lookup Zone abzubilden?

Die beiden Netze lassen sich zwar im IP-Adressraum zum Netz 188.95.234.0/23 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 innerhalb 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...