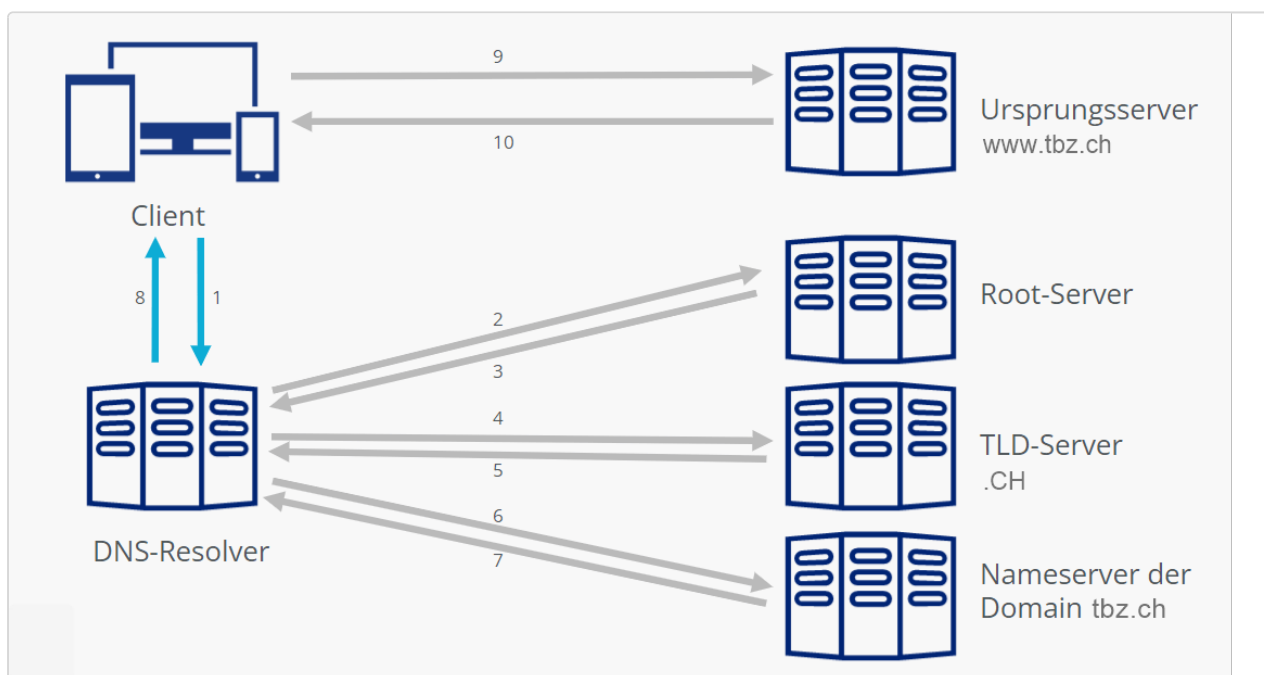


DNS-Auflösung

Wie Sie in der Übung [Die Hosts-Datei](#) herausgefunden haben, ist es nicht optimal, einen DNS-Dienst zentral zu betreiben. Dieser Server wäre viel zu anfällig und der Vorgang um Änderungen an einer DNS-Zone einzupflegen, wären verhältnismässig gross. Aus diesem Grund ist DNS als ein verteilter Dienst aufgebaut. DNS ist somit kein einzelner Server, sondern viele verschiedenen Server, welcher zusammenspielen, um die DNS-Auflösung zu ermöglichen.

Auftrag 1: Schauen Sie sich das untenstehende Schema an. Es zeigt auf wie eine DNS-Auflösung funktioniert.



Beschreibung Bild: Der **Client** möchte die IP-Adresse vom **Ursprungsserver von www.tbz.ch** wissen. Dazu stellt dieser eine Anfrage an seinem DNS-Resolver. Dieser kümmert sich für uns um die DNS-Auflösung und liefert uns am Ende das Resultat zurück.

Frage: In den vorangegangene Übungen haben Sie jeweils bereits DNS-Resolver verwendet und sogar öffentlich verfügbare DNS-Resolver in ihrem Betriebssystem hinterlegt. Was für DNS-Resolver kennen Sie?

Es gibt öffentliche DNS-Resolver wie die public Google DNS, Quad9, Switch DNS. Auf der anderen Seite haben Sie die DNS-Resolver, welche Ihnen Ihr ISP (Internet Service Provider, Swisscom, Sunrise) zur Verfügung stellt.

Der DNS-Resolver muss nun die Auskunft über die IP-Adresse zum Hostnamen bei verschiedenen DNS-Servern einholen.

Frage: Schauen Sie sich die drei verschiedenen Nameserver an, welche der DNS-Resolver nun fragen wird. Fällt Ihnen etwas auf, wenn Sie an die Übung mit dem FQDN zurückdenken?

Es gibt drei Nameserver, wobei wohl jeder für einen eigenen Teil der des FQDN zuständig ist.

- Root Nameserver für den Root der Doman
- TLD-Server für die Top-Level-Domain
- Domain-Name-Server für die Domain

Der DNS-Sever verteilt die Anfragen somit auf die einzelnen Teile des FQDN. Somit ist nicht ein einzelner Server für den ganzen Domain-Namen zuständig, sondern es ist eine verkettete Abfrage von verschiedenen DNS-Servern . Jeder DNS-Server ist dabei für einen kleinen Teil der ganzen Domain zuständig.

Wie im Ablauf ersichtlich ist, kontaktiert der DNS-Resolver als erstes die Root-Nameserver. Die Root-Nameserver sind eine fest definierte Liste die jeder DNS-Resolver hinterlegt hat. Der DNS-Resolver wird also als erstes immer einen dieser DNS-Server abfragen.

Nachfolgend finden Sie die Liste der Root-Server:

Servername	IP-Adresse	Betreiber
a.root-servers.net	198.41.0.4	Verisign, Inc.
b.root-servers.net	199.9.14.201	University of Southern California,
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53	US Army (Research Lab)
i.root-servers.net	192.36.148.17	Netnod, Inc.
j.root-servers.net	192.58.128.30	Verisign, Inc.
k.root-servers.net	193.0.14.129	RIPE NCC
l.root-servers.net	199.7.83.42	ICANN
m.root-servers.net	202.12.27.33	WIDE Project

Frage: Was fällt Ihnen auf, wenn Sie die Betreiber anschauen? Wie setzen sich die Betreiber zusammen? Warum ist nicht einfach nur ein Betreiber für alle Root-Nameserver zuständig?

Die Betreiber der Root-Nameserver sind zusammengesetzt auf öffentlichen Organisationen wie Universitäten, Gemeinnützigen Organisationen (ICANN, RIPE NCC), Regierungen (NASA, US Army, DoD) und privaten Firmen wie Verisign und Netnod.

Damit möchte man die Authentizität von DNS sicherstellen, weil viele verschiedenen Organisationen gemeinsam für die Root-Nameserver zuständig sind. Keine Organisation alleine sollte die Macht über das ganze DNS haben.

Die Root-Nameserver sind somit unser Einstiegspunkt des DNS-Resolvers. Sie können diese ebenfalls mit nslookup abfragen.

Auftrag 2: Öffnen Sie nslookup und stellen Sie eine Anfrage für tbz.ch an einen der oben stehenden Root-Nameserver. (Tipp. Sie haben in der Übung [nslookup](#) gelernt, wie Sie einen spezifischen DNS-

Server abfragen können). Sie sollten nun die untenstehende Antwort erhalten:

```
Name:      tbz. ch
Served by:
- b. nic. ch
    130. 59. 31. 43
    2001: 620: 0: ff: : 58
    ch
- f. nic. ch
    194. 146. 106. 10
    2001: 67c: 1010: 2: : 53
    ch
- e. nic. ch
    194. 0. 17. 1
    2001: 678: 3: : 1
    ch
- d. nic. ch
    194. 0. 25. 39
    2001: 678: 20: : 39
    ch
- a. nic. ch
    130. 59. 31. 41
    2001: 620: 0: ff: : 56
    ch
```

Frage: Schauen Sie sich nun erneut die Grafik mit dem Ablauf einer DNS-Abfrage an. Was könnten die die vom Root-Server erhaltene Antwort genau sein?

Der Root-Server schickt uns in der Antwort die zuständigen DNS-Server für die .CH Top-Level-Domain. Wir erhalten den Namen und die zugehörige IPv4 und IPv6 Adressen.

Frage: Was wird der DNS-Resolver mit diesen Informationen nun als nächstes machen?

Der DNS-Resolver schickt eine Anfrage an einen dieser Nameserver um den nächsten Teil des FQDN aufzulösen.

Auftrag 3: Stellen Sie nun eine DNS-Abfrage an einen der erhaltenen Top-Level-Domain Nameservern. Wie lautete der dazugehörige nslookup Befehl?

```
nslookup tbz.ch 130.59.31.4
```

Frage: Was erhalten Sie für eine Information in der Antwort vom Top-Level-Domain Nameserver?

Der Top-Level-Domain Nameserver gibt uns die Domain-Nameserver der Domain tbz.ch zurück:

```
nslookup tbz.ch a.nic.ch
```

```
Server: UnKnown
```

```
Address: 130.59.31.41
```

```
Name: tbz.ch
```

```
Served by:
```

```
- ns2.hosting.ch
```

```
193.223.77.3
```

```
tbz.ch
```

```
- ns1.hosting.ch
```

```
80.67.16.124
```

```
tbz.ch
```

Frage: Wie lauten die zuständigen Domain-Nameserver der Domain tbz.ch?

```
ns1.hosting.ch
```

```
ns2.hosting.ch
```

Frage: Was wird der DNS-Resolver mit diesen Informationen nun als nächstes machen?

Der DNS-Resolver schickt eine Anfrage an einen dieser Domain-Nameserver um den nächsten Teil des FQDN aufzulösen.

Auftrag 4: Stellen Sie nun eine DNS-Abfrage an einen der erhaltenen Top-Level-Domain Nameservern. Wie lautete der dazugehörige nslookup Befehl?

```
nslookup tbz.ch 193.223.77.3
```

Frage: Was haben Sie nun für eine Information in der Antwort vom Domain-Nameserver erhalten?

Der Domain-Nameserver hat uns nun die IP-Adresse von tbz.ch mitgeteilt.

Frage: Wie lautet die IP-Adresse von tbz.ch?

149.126.4.25

Auftrag 5: Wodurch unterscheidet sich diese Antwort von den bisherigen Antworten?

Wir haben keine weiteren DNS-Server mehr erhalten, sondern die finale Antwort mit der IP-Adresse. Die DNS-Auflösung ist für den Resolver damit nun beendet.

Frage: Was ist nun die letzte Aufgabe, welcher der DNS-Resolver macht?

Der DNS-Resolver übermittelt die Antwort zurück an den Client. Dieser kann nun mit der IP-Adresse den Server von tbz.ch erreichen.

Zusammenfassende Fragen

Frage: Beschreiben Sie in zwei bis drei Sätzen die Aufgaben und Eigenschaften von Root-Nameserver:

Die Root-Nameserver stellen den Einstiegspunkt in die DNS-Auflösung dar. Jeder DNS-Resolver kennt die Root-Nameserver, welche weltweit auf verschiedene Firmen und Organisation verteilt.

Frage: Beschreiben Sie in zwei bis drei Sätzen die Aufgaben und Eigenschaften von Top-Level-Nameserver:

Die Top-Level-Nameserver sind dafür zuständig, um einem DNS-Resolver die Nameserver der Domains unter dieser Top-Level-Domains zu liefern. Die Top-Level-Domains kennen somit alle Nameserver der Ihnen untergeordneten Domains.

Frage: Beschreiben Sie in zwei bis drei Sätzen die Aufgaben und Eigenschaften von Domain-Nameserver:

Die Domain-Nameserver enthalten die IP-Adressen der Hosts und Sub Domains unter der betreffenden Domain. Auf diesem Nameserver passt der Inhaber von tbz.ch seine DNS-Einträge an.

Frage: Überlegen Sie, was die Vorteile einer verteilten Lösung auf verschiedene Nameserver sein können:

- Die Last wird auf viele verschiedenen Nameserver verteilt.
- Der Inhaber einer DNS-Zone kann einfach auf einem Nameserver die Anpassung vornehmen. Diese wird dann automatisch weltweit verfügbar sein.

Weitere DNS-Auflösungen.

Auftrag 1: Führen Sie eine komplette DNS-Auflösung für die Domain `www.iten.io` durch. Notieren Sie alle beteiligten Nameserver:

Der DNS-Resolver fragt einen der Root-Nameserver:

```
a.root-servers.net 198.41.0.4
b.root-servers.net 199.9.14.201
c.root-servers.net 192.33.4.12
d.root-servers.net 199.7.91.13
u.s.w
```

Beispiel: nslookup `www.iten.io` 198.41.0.4

Die Root-Nameserver liefern folgende Antwort für den Top-Level-Domain Nameserver:

```
- b0.nic.io
    65.22.161.17
    2a01:8840:9f::17
    io
- a0.nic.io
    65.22.160.17
    2a01:8840:9e::17
    io
- a2.nic.io
    65.22.163.17
    2a01:8840:a1::17
    io
- c0.nic.io
```

```
65.22.162.17
2a01:8840:a0::17
io
```

Der DNS-Resolver fragt nun einen der erhaltenen TLD-Nameserver:

Beispiel: nslookup www.iten.io 65.22.161.17

```
Name:   www.iten.io
Served by:
- dns2.registrar-servers.com
      iten.io
- dns1.registrar-servers.com
      iten.io
```

Der DNS-Resolver fragt nun einen der erhaltenen Domain-Nameserver:

Beispiel: nslookup www.iten.io dns1.registrar-servers.com

```
Server: UnKnown
Address: 156.154.132.200
Name:   iten.io
Address: 80.74.136.2
Aliases: www.iten.io
```

Die IP-Adresse von www.iten.io lautet 80.74.136.2

Auftrag 2: Führen Sie eine komplette DNS-Auflösung für die Domain support.google.com durch.

Notieren Sie alle beteiligten Nameserver:

Der DNS-Resolver fragt einen der Root-Nameserver:

```
a.root-servers.net 198.41.0.4
b.root-servers.net 199.9.14.201
```

```
c.root-servers.net 192.33.4.12
d.root-servers.net 199.7.91.13
u.s.w
```

Beispiel: nslookup support.google.com 198.41.0.4

Die Root-Nameserver liefern folgende Antwort für den Top-Level-Domain Nameserver:

Name: support.google.com

Served by:

- e.gtld-servers.net

192.12.94.30

2001:502:1ca1::30

com

- b.gtld-servers.net

192.33.14.30

2001:503:231d::2:30

com

- j.gtld-servers.net

192.48.79.30

2001:502:7094::30

com

- m.gtld-servers.net

192.55.83.30

2001:501:b1f9::30

com

- i.gtld-servers.net

192.43.172.30

2001:503:39c1::30

com

- f.gtld-servers.net

192.35.51.30

2001:503:d414::30

com

```
- a.gtld-servers.net
    192.5.6.30
    2001:503:a83e::2:30
    com
- g.gtld-servers.net
    192.42.93.30
    2001:503:eea3::30
    com
- h.gtld-servers.net
    192.54.112.30
    2001:502:8cc::30
    com
- l.gtld-servers.net
    192.41.162.30
    2001:500:d937::30
    com
```

Der DNS-Resolver fragt nun einen der erhaltenen TLD-Nameserver:

Beispiel: nslookup support.google.com 192.12.94.30

```
Server: UnKnown
Address: 192.12.94.30
Name:   support.google.com
Served by:
- ns2.google.com
    2001:4860:4802:34::a
    216.239.34.10
    google.com
- ns1.google.com
    2001:4860:4802:32::a
    216.239.32.10
    google.com
- ns3.google.com
```

```
2001:4860:4802:36::a
216.239.36.10
google.com
- ns4.google.com
2001:4860:4802:38::a
216.239.38.10
google.com
```

Der DNS-Resolver fragt nun einen der erhaltenen Domain-Nameserver:

Beispiel: nslookup support.google.com 216.239.32.10

```
Server: ns1.google.com
Address: 216.239.32.10
Name: support.google.com
Addresses: 2a00:1450:400a:803::200e
172.217.168.78
```

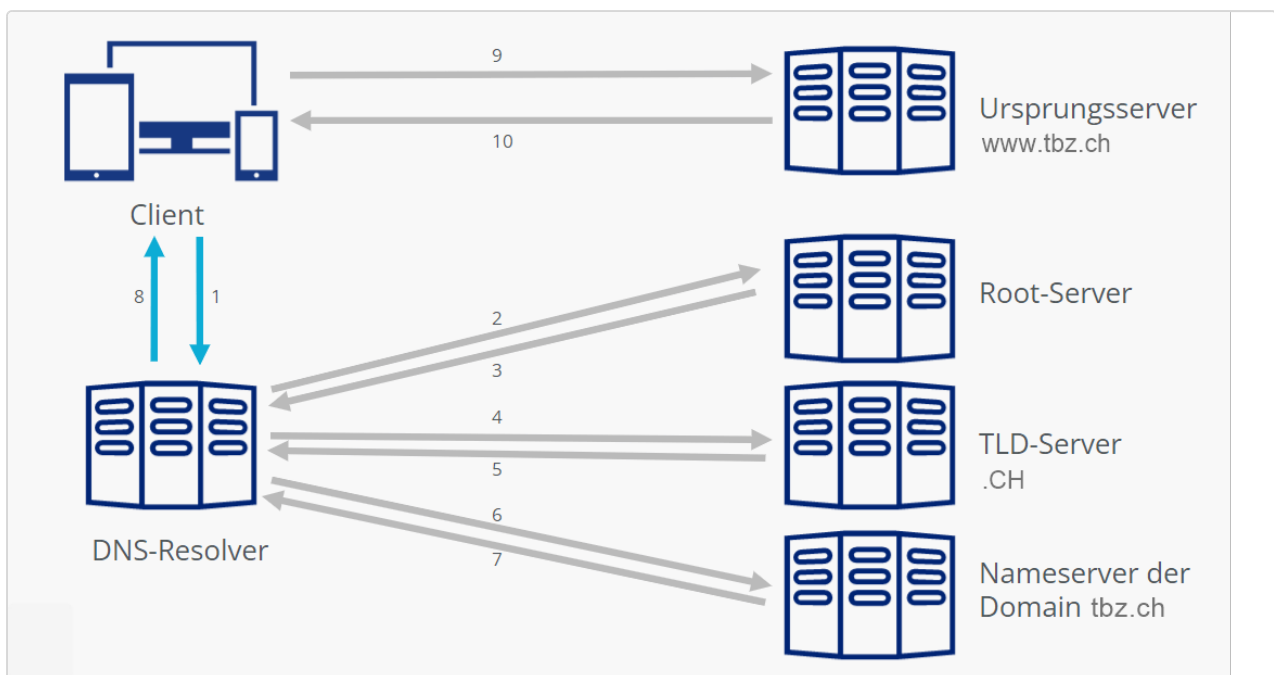
Die IP-Adresse von www.iten.io lautet 172.217.168.78

Rekursive und Iterative Abfragen

Eine DNS-Anfrage kann auf zwei Arten stattfinden:

- **Rekursive Abfrage:** Der fragende DNS-Server stellt einem anderen DNS-Server eine Anfrage und wartet, bis er eine vollständige Antwort inkl. IP-Adresse erhält. Der andere DNS-Server kümmert sich vollständig um die DNS-Abfrage.
- **Iterative Abfrage:** der fragende DNS-Server stellt einem anderen DNS-Server eine Anfrage, erhält einen Verweis auf anderen zuständigen Nameserver, und stellt dann bei diesem Nameserver eine weitere Anfrage. Dies macht der fragende DNS-Server solange, bis er einen DNS-Server findet, der eine IP-Adresse zurück liefert.

Auftrag 1: In einer regulären DNS-Auflösung kommen in der Regel beide Varianten zum Einsatz. Studieren Sie den DNS-Ablauf erneut und beurteilen Sie, bei welchen Abfragen (1 - 10) es sich um rekursive Abfrage, iterative Abfragen und gar keine DNS-Abfragen handelt:



Iterative Abfragen: 2, 3, 4, 5, 6, 7

Rekursive Abfragen: 1, 8

Keine DNS-Abfragen: 9, 10

Auftrag 2: Vervollständigen Sie folgende Sätze:

Wenn der DNS-Client eine Abfrage dem DNS-Resolver stellt und wartet bis der DNS-Resolver die IP-Adresse der Domain liefert, dann handelt es sich um eine **rekursive** DNS-Abfrage.

Wenn ich mit nslookup direkt bei einem DNS-Server eine Anfrage stelle, dann handelt es sich um eine **iterative** DNS-Abfrage.

Daraus resultiert, dass wir die finale Antwort von zwei Arten von Nameservern erhalten können. Eine direkt vom zuständigen Nameserver der betreffenden Domain oder eine von einem Resolver, der die Abfragen für uns übernimmt.

Auftrag 3: Überprüfen Sie den Unterschied der beiden Antwort-Typen mit nslookup.

Fragen Sie als erstes einen öffentlichen DNS-Resolver. Dadurch führen Sie eine rekursive Anfrage aus:

```
nslookup www.tbz.ch 8.8.8.8
```

Nun führen Sie in einem weiteren CMD-Fenster eine direkt Anfrage an den zuständigen Domain-Nameserver aus. Dadurch führen Sie eine iterative Anfrage aus:

```
nslookup www.tbz.ch 80.67.16.124
```

Frage: Was für einen Unterschied fällt Ihnen auf?

Bei der rekursiven Antwort erhalten wir ein nicht autorisierende Antwort. Bei der direkten iterativen Abfrage erhalten wir diesen Hinweis nicht. Es ist somit eine autorisierte Antwort.

Frage: Was sagt uns die Information, dass es sich um eine autorisierende Antwort handelt?

Die Antwort dieser DNS-Abfrage stammt vom zuständigen Nameserver der diese Domain verwaltet. Es ist keine Antwort, die über einen dritten Nameserver weitergereicht wurde.

Revision #4

Created 8 December 2022 00:33:34 by Admin

Updated 26 January 2023 00:04:28 by Admin