Domain Name System (DNS)

IT-Technik Netzwerkgrundlagen

Sebastian Meisel

8. März 2023

1 Domain Name System (DNS)

DNS ist ein Dienst der die aktuell zu einer **Full Qualified Domain (FQD)** gehörende **IP-Adresse** zuordnet. Dies geschieht über eine hierarchisch aufgebaute Struktur von **DNS-Servern**, die Informationen zu den **FQDs** speichern.

1.1 Was ist ein Full Qualified Domain (FQD)?

Eine **FQD** ist ein Bestandteil jeder *URL*, die einen Computer bezeichnet, auf dem eine bestimmte *Ressource* (z. B. eine Webseite, eine Email-Adresse, ein FTP-Verzeichnis) befindet.

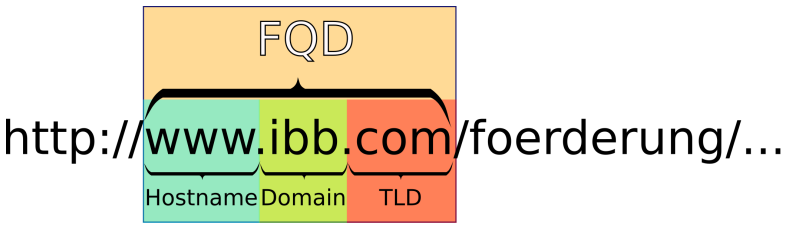

Abbildung 1: Uniform Ressource Locator mit Full Qualified Domain

1.1.1 Root

DNS-Server lösen **FDQs** von Links nach rechts auf. Ganz links beginnt die Adresse mit einen Punkt, der aber in der Regel ausgelassen wird. Dieser steht für die ”Wurzel die **Root** - die die oberste Ebene in der Hierarchie der Nameserver darstellt.
Für jede dieser Ebenen gibt es mehrere **authoritative Nameserver**. Für die Wurzel sind das die 13 Root-Nameserver, die nach dem Schema `<Buchstabe>.root-servers.net` benannt sind.
Der Linuxbefehl `dig` ermöglicht es einen spezifischen Nameserver anzufragen. Die folgenden Eingabe fragt den dritten Root-Nameserver nach den für die durch einen Punkt repräsentierte **Root**.

```
dig @c.root-servers.net .
```

Die Antwort enthält zunächst die **FQDs** aller Root-Nameserver und danach deren *A-Records* (= IPv4-Adressen) und *AAAA-Records* (= IPv6 Adressen):

```
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> @a.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45193
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
. 518400 IN NS e.root-servers.net.
. 518400 IN NS h.root-servers.net.
. 518400 IN NS l.root-servers.net.
. 518400 IN NS i.root-servers.net.
. 518400 IN NS a.root-servers.net.
. 518400 IN NS d.root-servers.net.
. 518400 IN NS c.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS j.root-servers.net.
. 518400 IN NS k.root-servers.net.
. 518400 IN NS g.root-servers.net.
. 518400 IN NS m.root-servers.net.
. 518400 IN NS f.root-servers.net.

;; ADDITIONAL SECTION:
e.root-servers.net. 518400 IN A 192.203.230.10
e.root-servers.net. 518400 IN AAAA 2001:500:a8::e
h.root-servers.net. 518400 IN A 198.97.190.53
h.root-servers.net. 518400 IN AAAA 2001:500:1::53
l.root-servers.net. 518400 IN A 199.7.83.42
l.root-servers.net. 518400 IN AAAA 2001:500:9f::42
i.root-servers.net. 518400 IN A 192.36.148.17
i.root-servers.net. 518400 IN AAAA 2001:7fe::53
a.root-servers.net. 518400 IN A 198.41.0.4
```

```
a.root-servers.net. 518400 IN AAAA 2001:503:ba3e::2:30
d.root-servers.net. 518400 IN A 199.7.91.13
d.root-servers.net. 518400 IN AAAA 2001:500:2d::d
c.root-servers.net. 518400 IN A 192.33.4.12
c.root-servers.net. 518400 IN AAAA 2001:500:2::c
b.root-servers.net. 518400 IN A 199.9.14.201
b.root-servers.net. 518400 IN AAAA 2001:500:200::b
j.root-servers.net. 518400 IN A 192.58.128.30
j.root-servers.net. 518400 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 518400 IN A 193.0.14.129
k.root-servers.net. 518400 IN AAAA 2001:7fd::1
g.root-servers.net. 518400 IN A 192.112.36.4
g.root-servers.net. 518400 IN AAAA 2001:500:12::d0d
m.root-servers.net. 518400 IN A 202.12.27.33
m.root-servers.net. 518400 IN AAAA 2001:dc3::35
f.root-servers.net. 518400 IN A 192.5.5.241
f.root-servers.net. 518400 IN AAAA 2001:500:2f::f

;; Query time: 63 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Mon Jan 23 20:24:05 CET 2023
;; MSG SIZE  rcvd: 811
```

1.1.2 Top-Level-Domain (TLD)

Die nächste Ebene unterhalb der **Root** stellen die **TLDs** dar. Diese stellen eine Art Grobeinteilung des Internets dar und werden von der *Internet Assigned Numbers Authority (IANA)* vergeben.
Neben **länderspezifischen TLDs**, wie `de.` (Deutschland) oder `uk.` (United Kingdom) gibt es noch allgemeine *generic TLDs*, wie `com.` für kommerzielle Angebote oder `edu.` für Bildungsangebote.
Die authoritativen Nameserver der TLDs kann man bei den Root-Nameservern erfragen:

```
dig @c.root-servers.net com.

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> @a.root-servers.net com.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13021
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;com. IN A

;; AUTHORITY SECTION:
com. 172800 IN NS e.gtld-servers.net.
com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS m.gtld-servers.net.
com. 172800 IN NS i.gtld-servers.net.
com. 172800 IN NS f.gtld-servers.net.
com. 172800 IN NS a.gtld-servers.net.
com. 172800 IN NS g.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS l.gtld-servers.net.
com. 172800 IN NS k.gtld-servers.net.
com. 172800 IN NS c.gtld-servers.net.
com. 172800 IN NS d.gtld-servers.net.

;; ADDITIONAL SECTION:
e.gtld-servers.net. 172800 IN A 192.12.94.30
e.gtld-servers.net. 172800 IN AAAA 2001:502:1ca1::30
b.gtld-servers.net. 172800 IN A 192.33.14.30
b.gtld-servers.net. 172800 IN AAAA 2001:503:231d::2:30
j.gtld-servers.net. 172800 IN A 192.48.79.30
j.gtld-servers.net. 172800 IN AAAA 2001:502:7094::30
m.gtld-servers.net. 172800 IN A 192.55.83.30
m.gtld-servers.net. 172800 IN AAAA 2001:501:b1f9::30
i.gtld-servers.net. 172800 IN A 192.43.172.30
i.gtld-servers.net. 172800 IN AAAA 2001:503:39c1::30
f.gtld-servers.net. 172800 IN A 192.35.51.30
f.gtld-servers.net. 172800 IN AAAA 2001:503:d414::30
a.gtld-servers.net. 172800 IN A 192.5.6.30
a.gtld-servers.net. 172800 IN AAAA 2001:503:a83e::2:30
g.gtld-servers.net. 172800 IN A 192.42.93.30
g.gtld-servers.net. 172800 IN AAAA 2001:503:eea3::30
h.gtld-servers.net. 172800 IN A 192.54.112.30
h.gtld-servers.net. 172800 IN AAAA 2001:502:8cc::30
l.gtld-servers.net. 172800 IN A 192.41.162.30
l.gtld-servers.net. 172800 IN AAAA 2001:500:d937::30
k.gtld-servers.net. 172800 IN A 192.52.178.30
```

```
k.gtld-servers.net. 172800 IN AAAA 2001:503:d2d::30
c.gtld-servers.net. 172800 IN A 192.26.92.30
c.gtld-servers.net. 172800 IN AAAA 2001:503:83eb::30
d.gtld-servers.net. 172800 IN A 192.31.80.30
d.gtld-servers.net. 172800 IN AAAA 2001:500:856e::30

;; Query time: 71 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Mon Jan 23 20:57:32 CET 2023
;; MSG SIZE  rcvd: 828
```

In einigen Ländern gibt es auch verbindliche *Second-Level-Domains*, z. B. in Großbritanien. Dort gibt es etwa `gov.uk.` für Regierungsseiten, oder `co.uk.` für kommerzielle Seiten:

```
dig @nsd.nic.uk. co.uk.
```

1.1.3 Domainname

Die nächste Ebene stellen die frei wählbaren **Domains** dar, die z. B. für ein Unternehmen (z. B. `google.com.`) stehen. Diese müssen kostenpflichtig registriert werden. Außerdem muss für jede *Domain* wiederum mindestens ein *autoritativer Nameserver* betrieben werden.

```
dig @k.gtld-servers.net. ibb.com.

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> @k.gtld-servers.net. ibb.com.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17024
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ibb.com. IN A

;; AUTHORITY SECTION:
ibb.com. 172800 IN NS ns1.inexio.net.
ibb.com. 172800 IN NS ns2.inexio.net.
ibb.com. 172800 IN NS ns3.inexio.net.

;; Query time: 63 msec
```

```
;; SERVER: 192.52.178.30#53(k.gtld-servers.net.) (UDP)
;; WHEN: Mon Jan 23 21:14:43 CET 2023
;; MSG SIZE  rcvd: 100
```

1.1.4 Hostname

Jeder Rechner innerhalb der Domain hat einen Hostname. Der Standard für Webserver ist dabei der Hostname `www.`, dieser wird angenommen, wenn kein Hostname angenommen wurde. Prinzipiell ist der Hostname frei wählbar und es können beliebig viele Hostnamen pro Domain definiert werden. Die **IP** des **Hosts** ist nur den **autoritativen Nameservern** der **Domain** bekannt.

```
dig @ns1.inexio.net. www.ibb.com.
```

```
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> @ns1.inexio.net. www.ibb.com.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60922
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 7
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4f99e55789d034c13339254463ceececa266b389a5b2641b (good)
;; QUESTION SECTION:
;www.ibb.com. IN A

;; ANSWER SECTION:
www.ibb.com. 3600 IN A 136.243.235.86

;; AUTHORITY SECTION:
ibb.com. 3600 IN NS ns2.inexio.net.
ibb.com. 3600 IN NS ns1.inexio.net.
ibb.com. 3600 IN NS ns3.inexio.net.

;; ADDITIONAL SECTION:
ns1.inexio.net. 86400 IN A 131.117.146.40
ns2.inexio.net. 86400 IN A 188.210.43.194
ns3.inexio.net. 86400 IN A 149.6.67.219
ns1.inexio.net. 86400 IN AAAA 2a01:5c0:6:38::40
ns2.inexio.net. 86400 IN AAAA 2a01:5c0:6:8::194
ns3.inexio.net. 86400 IN AAAA 2001:978:2:4c::e:3
```

```
;; Query time: 47 msec
;; SERVER: 131.117.146.40#53(ns1.inexio.net.) (UDP)
;; WHEN: Mon Jan 23 21:24:12 CET 2023
;; MSG SIZE  rcvd: 280
```

2 DNS-Cache-Server

Jede Antwort eines *Nameservers* hat eine feste Gültigkeit, die sogenannte *Time To Live (TTL)*. Diese wird in Sekunden angegeben.
In jeder Domain und auf jedem Rechner wird ein **DNS-Cache** betrieben in dem bekannte Adressen für die **TTL** zwischenspeichert. Unbekannte oder abgelaufene Adressen werden dann wiederum von einem öffentlichen **DNS-Cache-Server** erfragt. Solche Cache-Server werden von großen Unternehmen, wie Google (`8.8.8.8`, `4.4.4.4`) oder Cloudflare (`1.1.1.1`, `1.0.0.1`) betrieben.

3 DNS over TLS (DoT) / HTTPS (DoH) / QUIC (DoQ)

Während Webseiten heute in der Regel *verschlüsselt* übertragen werden, arbeitet das DNS-Protokoll unverschlüsselt. Damit beleibt verfolgbar, welche Seiten ein Teilnehmer besucht, auch wenn er diese verschlüsselt abruft.
Dies sollen die verschlüsselten DNS-Protokolle **DoT**, **DoH** und **DoQ** ändern. Diese Technik setzt sich aber nur langsam durch, u. a. weil sie bewährte Sicherheitstechniken, die auf DNS-Blocking (dem Sperren von DNS-Abfragen auf bestimmte Adressen, die z. B. Schadsoftware verbreiten) aufbauen, verhindern.