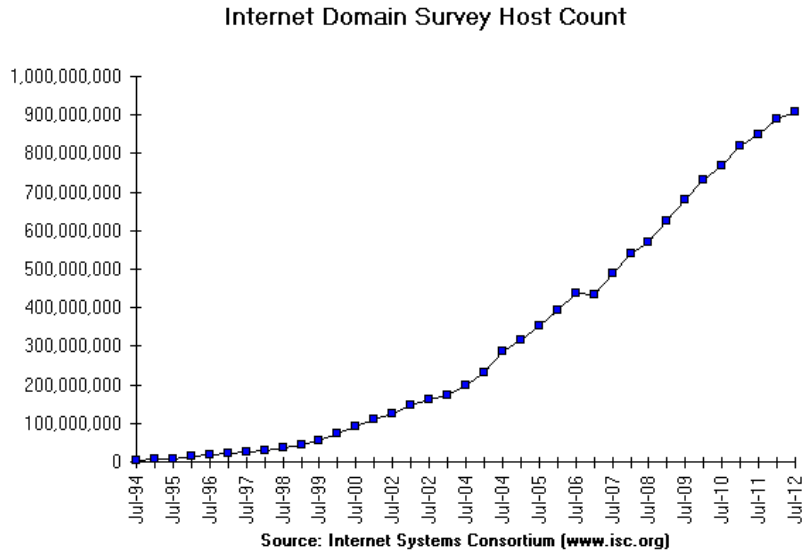
DNS – Domain Name Service

DNS übersetzt verwendete Rechnernamen in numerische IP-Adressen (forward lookup www.wu-wien.ac.at -> 137.208.3.82) und umgekehrt (reverse lookup 137.208.3.82 -> www.wu-wien.ac.at). In den Anfangstagen des Internets konnte jeder Standort eine eigene Rechnertabelle mit den Hostname und IP-Adressen aller Internet-Rechner halten.

Bei inzwischen Millionen angeschlossener Rechner ist diese Vorgehensweise nicht mehr möglich und sinnvoll, stattdessen wird das Domain Name Service – DNS verwendet.



Quelle: https://www.isc.org/solutions/survey

Lokale Tabellen werden auch weiterhin verwendet, ein Beispiel für eine lokale Rechnertabelle auf eine UNIX-Rechner: /etc/hosts

```
root@webduxv91:~# cat /etc/hosts


127.0.0.1               localhost
173.252.101.26          www.facebook.com
194.116.243.20          www.derstandard.at
```

Um das DNS Service nutzen zu können, wird zumindest eine IP-Adresse eines DNS-Servers eingetragen bzw. können diese Adressen dynamisch (per DHCP) oder nach erfolgter Authentifizierung per PPP/PPTP etc. automatisch zugewiesen werden

Beispiel für statische DNS-Clienteinstellungen: /etc/resolv.conf

```
root@webduxv91:~# cat /etc/resolv.conf

nameserver 195.3.86.139
nameserver 213.33.76.25
```

Festlegen der Suchreihenfolge – /etc/hosts oder Resolver

```
root@webduxv91:~# cat /etc/nsswitch.conf

hosts:      files dns
```

DNS wurde 1983 von Paul Mockapetris entworfen und in RFC 882 und 883 beschrieben. (Beide wurden inzwischen von RFC 1034 und RFC 1035 abgelöst und durch zahlreiche weitere Standards ergänzt).

RFC -> http://tools.ietf.org

Hauptmerkmal von DNS ist

- Hierarchischer Aufbau
- Dezentrale Verwaltung

Verwendet werden die Protokolle UDP und TCP, Port 53

Unterschieden werden:

- Resolver – holen sich die Einträge und geben diese weiter
- Authoritative – haben selbst die notwendigen Infos

DNS-Anfragen werden normalerweise per UDP Port 53 zum Nameserver gesendet. Der DNS-Standard erlaubt aber auch TCP. Zonentransfers werden stets über Port 53 TCP durchgeführt.

Hierachischer Aufbau

. (Root-Zone)
 at (Top-Level-Domain)
  ac.at.
   wu-wien.ac.at. -> www.wu-wien.ac.at.
  gv.at. (Second-Level-Domain)
  co.at. (Second-Level-Domain)
 de. (Top-Level-Domain)
 com. (Top-Level-Domain)
 net. (Top-Level-Domain)
 org. (Top-Level-Domain)

An ihrer oberster Stelle steht die Root-Zone „.“. Diese Datei besteht aus ca. 2500 Einträgen und ist die Wurzel. Sie enthält die Namen und IP-Adressen der für die Top-Level-Domainen zuständigen Nameserver und besteht derzeit aus 13 Servern

Ein Resolver muss zumindest diese 13 Server „kennen“

Aktuelles root.hint-File - http://www.iana.org/domains/root/files:

```
; formerly NS.INTERNIC.NET
;
.                        3600000      IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.                        3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.                        3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A     192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                        3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A     128.63.2.53
H.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.                        3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.                        3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FD::1
;
; OPERATED BY ICANN
;
.                        3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:3::42
;
; OPERATED BY WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.      3600000      AAAA  2001:DC3::35
; End of File
```

Einige der Root-Name-Server bestehen jedoch nicht aus einem, sondern mehreren Rechnern, die zu einem logischen Server zusammengeschlossen sind. Diese Rechner (*Nodes*) befinden sich an verschiedenen Standorten um die ganze Welt und sind per „Anycast“ über dieselbe IP-Adresse erreichbar.

Quelle: https://www.isc.org/community/f-root

„Anycast“ wird ein einer anderen Einheit genau besprochen werden!

Top Level Domains:

Top Level Domains (TLD) unterscheiden sich in:

- Country Code Domains (.at, .de, .ch, .us, etc.)
- Generic Domains (.aero, .asia, .biz, .cat, .com, .coop, .edu, .gov, .info, .jobs, .mobi, .int, .mil, .museum, .name, .net, .org, .pro, .tel and .travel)
- Infrastructure Domain (.arpa) – verwendet fuer Reverse Lookup Zonen

Weitere Infos unter http://www.iana.org (Internet Assigned Numbers Authority), http://www.icann.org (Internet Corporation for Assigned Names and Numbers)

Abfragen:

Ein Nameserver kann eine Anfrage wie folgt beantworten:

- **autoritativ** (der Server holt die Daten aus einer lokalen Zonendatei)
- nicht-autoritativ (Resolver)
    - **rekursiv** (der Server holt die Daten von anderen Nameserver)
    - **iterativ** (Serverantwort mit Verweis auf andere Nameserver)

Im rekursiven Modus schickt der Resolver eine **rekursive Anfrage** an den ihm zugeordneten Server. Hat dieser die gewünschte Information nicht im eigenen Datenbestand, so kontaktiert der Server weitere Nameserver, und zwar solange bis er entweder eine positive oder negative Antwort von einem autoritativen Server erhält.

Bei einer **iterativen Anfrage** bekommt der Nameserver entweder den gewünschten Resource Record oder einen Verweis auf weitere Nameserver, die er als nächstes fragt. Der Nameserver

hangelt sich so von Nameserver zu Nameserver bis er von einem eine verbindliche Antwort erhält.

```
root@webduxv91:~# host -avn www.orf.at F.ROOT-SERVERS.NET
Trying "www.orf.at"
Using domain server:
Name: F.ROOT-SERVERS.NET
Address: 192.5.5.241#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30776
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 14

;; QUESTION SECTION:
;www.orf.at.                    IN      ANY

;; AUTHORITY SECTION:
at.                     172800  IN      NS      n.ns.at.
at.                     172800  IN      NS      r.ns.at.
at.                     172800  IN      NS      ns1.univie.ac.at.
at.                     172800  IN      NS      u.ns.at.
at.                     172800  IN      NS      d.ns.at.
at.                     172800  IN      NS      ns9.univie.ac.at.
at.                     172800  IN      NS      ns2.univie.ac.at.
at.                     172800  IN      NS      j.ns.at.

;; ADDITIONAL SECTION:
d.ns.at.                172800  IN      A       81.91.161.98
j.ns.at.                172800  IN      A       194.146.106.50
n.ns.at.                172800  IN      A       87.233.175.130
r.ns.at.                172800  IN      A       194.0.25.10
u.ns.at.                172800  IN      A       195.66.241.82
ns1.univie.ac.at.       172800  IN      A       78.104.144.2
ns2.univie.ac.at.       172800  IN      A       192.92.125.2
ns9.univie.ac.at.       172800  IN      A       194.0.10.100
d.ns.at.                172800  IN      AAAA    2a02:568:20:1::d
j.ns.at.                172800  IN      AAAA    2001:67c:1010:12::53
r.ns.at.                172800  IN      AAAA    2001:67c:1bc::10
ns1.univie.ac.at.       172800  IN      AAAA    2001:628:2030:4301::2
ns2.univie.ac.at.       172800  IN      AAAA    2001:678:1c::2
ns9.univie.ac.at.       172800  IN      AAAA    2001:678:d::cafe

Received 471 bytes from 192.5.5.241#53 in 177 ms
```

Größere Internet Service Provider trennen die Autoritativen DNS-Server von den Nicht-Autoritativen-DNS-Server:

DNS-Server (A1-Business):

- Resolver (DSN-Server für Kundenabfragen): 195.3.86.139, 213.33.76.25
- ZonenServer: dns1.telekom.at, dns2.telekom.at, dns3.telekom.at

Resolver: IP für www.wu-wien.ac.at ermitteln:

Ermitteln der DNS-Server für die .at-Domaine (iterative Anfrage über Root Name Server):

```
root@webduxv91:~# host -t ns -v .
Trying "."
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48320
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       82672   IN      NS      a.root-servers.net.
.                       82672   IN      NS      b.root-servers.net.
.                       82672   IN      NS      c.root-servers.net.
.                       82672   IN      NS      d.root-servers.net.
.                       82672   IN      NS      e.root-servers.net.
.                       82672   IN      NS      f.root-servers.net.
.                       82672   IN      NS      g.root-servers.net.
.                       82672   IN      NS      h.root-servers.net.
.                       82672   IN      NS      i.root-servers.net.
.                       82672   IN      NS      j.root-servers.net.
.                       82672   IN      NS      k.root-servers.net.
.                       82672   IN      NS      l.root-servers.net.
.                       82672   IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3596272 IN      A       198.41.0.4
a.root-servers.net.     3596272 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3596272 IN      A       192.228.79.201
c.root-servers.net.     3596272 IN      A       192.33.4.12
d.root-servers.net.     3555435 IN      A       199.7.91.13
d.root-servers.net.     3596272 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3596272 IN      A       192.203.230.10
f.root-servers.net.     3596272 IN      A       192.5.5.241
f.root-servers.net.     3596272 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3596272 IN      A       192.112.36.4
h.root-servers.net.     3596272 IN      A       128.63.2.53
h.root-servers.net.     3596272 IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     3596272 IN      A       192.36.148.17
i.root-servers.net.     3596272 IN      AAAA    2001:7fe::53

Received 512 bytes from 195.3.86.139#53 in 2 ms
```

Bzw:

```
root@webduxv91:~# dig ns .

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1 <<>> ns .
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51595
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       82645   IN      NS      a.root-servers.net.
.                       82645   IN      NS      b.root-servers.net.
.                       82645   IN      NS      c.root-servers.net.
.                       82645   IN      NS      d.root-servers.net.
.                       82645   IN      NS      e.root-servers.net.
.                       82645   IN      NS      f.root-servers.net.
.                       82645   IN      NS      g.root-servers.net.
.                       82645   IN      NS      h.root-servers.net.
.                       82645   IN      NS      i.root-servers.net.
.                       82645   IN      NS      j.root-servers.net.
.                       82645   IN      NS      k.root-servers.net.
.                       82645   IN      NS      l.root-servers.net.
.                       82645   IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3596245 IN      A       198.41.0.4
a.root-servers.net.     3596245 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3596245 IN      A       192.228.79.201
```

```
c.root-servers.net.     3596245 IN      A       192.33.4.12
d.root-servers.net.     3555408 IN      A       199.7.91.13
d.root-servers.net.     3596245 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3596245 IN      A       192.203.230.10
f.root-servers.net.     3596245 IN      A       192.5.5.241
f.root-servers.net.     3596245 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3596245 IN      A       192.112.36.4
h.root-servers.net.     3596245 IN      A       128.63.2.53
h.root-servers.net.     3596245 IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     3596245 IN      A       192.36.148.17
i.root-servers.net.     3596245 IN      AAAA    2001:7fe::53

;; Query time: 2 msec
;; SERVER: 195.3.86.139#53(195.3.86.139)
;; WHEN: Mon May 13 16:18:53 2013
;; MSG SIZE  rcvd: 512
```

Abfrage, der TLD für .at.:

```
root@webduxv91:~# host -t ns -v  at.
Trying "at"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43472
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 11

;; QUESTION SECTION:
;at.                            IN      NS

;; ANSWER SECTION:
at.                     86387   IN      NS      ns1.univie.ac.at.
at.                     86387   IN      NS      ns9.univie.ac.at.
at.                     86387   IN      NS      ns2.univie.ac.at.
at.                     86387   IN      NS      d.ns.at.
at.                     86387   IN      NS      j.ns.at.
at.                     86387   IN      NS      n.ns.at.
at.                     86387   IN      NS      r.ns.at.
at.                     86387   IN      NS      u.ns.at.

;; ADDITIONAL SECTION:
ns1.univie.ac.at.       43      IN      A       78.104.144.2
ns9.univie.ac.at.       583     IN      A       194.0.10.100
ns2.univie.ac.at.       563     IN      A       192.92.125.2
d.ns.at.                172787  IN      A       81.91.161.98
j.ns.at.                172787  IN      A       194.146.106.50
n.ns.at.                172787  IN      A       87.233.175.130
r.ns.at.                172787  IN      A       194.0.25.10
u.ns.at.                172787  IN      A       195.66.241.82
ns1.univie.ac.at.       10787   IN      AAAA    2001:628:2030:4301::2
ns9.univie.ac.at.       172787  IN      AAAA    2001:678:d::cafe
ns2.univie.ac.at.       10787   IN      AAAA    2001:678:1c::2

Received 379 bytes from 195.3.86.139#53 in 1 ms
```

Bzw:

```
root@webduxv91:~# dig ns at.

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1 <<>> ns at.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33122
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 11

;; QUESTION SECTION:
;at.                            IN      NS

;; ANSWER SECTION:
at.                     86364   IN      NS      ns1.univie.ac.at.
at.                     86364   IN      NS      ns9.univie.ac.at.
at.                     86364   IN      NS      ns2.univie.ac.at.
at.                     86364   IN      NS      d.ns.at.
at.                     86364   IN      NS      j.ns.at.
at.                     86364   IN      NS      n.ns.at.
at.                     86364   IN      NS      r.ns.at.
at.                     86364   IN      NS      u.ns.at.
```

```
;; ADDITIONAL SECTION:
ns1.univie.ac.at.       20      IN      A       78.104.144.2
ns9.univie.ac.at.       560     IN      A       194.0.10.100
ns2.univie.ac.at.       540     IN      A       192.92.125.2
d.ns.at.                172764  IN      A       81.91.161.98
j.ns.at.                172764  IN      A       194.146.106.50
n.ns.at.                172764  IN      A       87.233.175.130
r.ns.at.                172764  IN      A       194.0.25.10
u.ns.at.                172764  IN      A       195.66.241.82
ns1.univie.ac.at.       10764   IN      AAAA    2001:628:2030:4301::2
ns9.univie.ac.at.       172764  IN      AAAA    2001:678:d::cafe
ns2.univie.ac.at.       10764   IN      AAAA    2001:678:1c::2

;; Query time: 1 msec
;; SERVER: 195.3.86.139#53(195.3.86.139)
;; WHEN: Mon May 13 16:20:02 2013
;; MSG SIZE  rcvd: 379
```

Abfrage DNS-Server für ac.at.:

```
root@webduxv91:~# host -t ns -v  ac.at.
Trying "ac.at"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31040
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ac.at.                         IN      NS

;; ANSWER SECTION:
ac.at.                  10800   IN      NS      n.nic.at.
ac.at.                  10800   IN      NS      ns2.univie.ac.at.
ac.at.                  10800   IN      NS      d.nic.at.
ac.at.                  10800   IN      NS      ns1.univie.ac.at.

Received 102 bytes from 195.3.86.139#53 in 5 ms
```

Bzw:

```
root@webduxv91:~# dig ns ac.at.

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1 <<>> ns ac.at.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56440
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ac.at.                         IN      NS

;; ANSWER SECTION:
ac.at.                  10786   IN      NS      n.nic.at.
ac.at.                  10786   IN      NS      ns2.univie.ac.at.
ac.at.                  10786   IN      NS      d.nic.at.
ac.at.                  10786   IN      NS      ns1.univie.ac.at.

;; Query time: 2 msec
;; SERVER: 195.3.86.139#53(195.3.86.139)
;; WHEN: Mon May 13 16:20:43 2013
;; MSG SIZE  rcvd: 102
```

Für Domaine “wu-wien.ac.at”:

```
root@webduxv91:~# host -t ns -v  wu-wien.ac.at.
Trying "wu-wien.ac.at"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33230
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;wu-wien.ac.at.                 IN      NS

;; ANSWER SECTION:
```

```
wu-wien.ac.at.          600     IN      NS      ns2.wu-wien.ac.at.
wu-wien.ac.at.          600     IN      NS      ns1.wu-wien.ac.at.
wu-wien.ac.at.          600     IN      NS      ns5.univie.ac.at.

;; ADDITIONAL SECTION:
ns1.wu-wien.ac.at.      208     IN      A       137.208.10.10
ns2.wu-wien.ac.at.      208     IN      A       137.208.20.10

Received 124 bytes from 195.3.86.139#53 in 5 ms
```

Bzw:

```
root@webduxv91:~# dig ns wu-wien.ac.at.

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1 <<>> ns wu-wien.ac.at.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46037
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;wu-wien.ac.at.                 IN      NS

;; ANSWER SECTION:
wu-wien.ac.at.          583     IN      NS      ns2.wu-wien.ac.at.
wu-wien.ac.at.          583     IN      NS      ns1.wu-wien.ac.at.
wu-wien.ac.at.          583     IN      NS      ns5.univie.ac.at.

;; ADDITIONAL SECTION:
ns1.wu-wien.ac.at.      191     IN      A       137.208.10.10
ns2.wu-wien.ac.at.      191     IN      A       137.208.20.10

;; Query time: 2 msec
;; SERVER: 195.3.86.139#53(195.3.86.139)
;; WHEN: Mon May 13 16:21:19 2013
;; MSG SIZE  rcvd: 124
```

IP-Adresse für www.wu-wien.ac.at:

```
root@webduxv91:~# host -t a -v  www.wu-wien.ac.at.
Trying "www.wu-wien.ac.at"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12333
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 2

;; QUESTION SECTION:
;www.wu-wien.ac.at.             IN      A

;; ANSWER SECTION:
www.wu-wien.ac.at.      600     IN      A       137.208.3.113
www.wu-wien.ac.at.      600     IN      A       137.208.3.114
www.wu-wien.ac.at.      600     IN      A       137.208.3.112

;; AUTHORITY SECTION:
wu-wien.ac.at.          600     IN      NS      ns2.wu-wien.ac.at.
wu-wien.ac.at.          600     IN      NS      ns5.univie.ac.at.
wu-wien.ac.at.          600     IN      NS      ns1.wu-wien.ac.at.

;; ADDITIONAL SECTION:
ns1.wu-wien.ac.at.      162     IN      A       137.208.10.10
ns2.wu-wien.ac.at.      162     IN      A       137.208.20.10

Received 176 bytes from 195.3.86.139#53 in 6 ms
```

Bzw:

```
root@webduxv91:~# dig a www.wu-wien.ac.at.

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1 <<>> a www.wu-wien.ac.at.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65121
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 2
```

```
;; QUESTION SECTION:
;www.wu-wien.ac.at.             IN      A

;; ANSWER SECTION:
www.wu-wien.ac.at.      577     IN      A       137.208.3.113
www.wu-wien.ac.at.      577     IN      A       137.208.3.114
www.wu-wien.ac.at.      577     IN      A       137.208.3.112

;; AUTHORITY SECTION:
wu-wien.ac.at.          531     IN      NS      ns2.wu-wien.ac.at.
wu-wien.ac.at.          531     IN      NS      ns1.wu-wien.ac.at.
wu-wien.ac.at.          531     IN      NS      ns5.univie.ac.at.

;; ADDITIONAL SECTION:
ns1.wu-wien.ac.at.      139     IN      A       137.208.10.10
ns2.wu-wien.ac.at.      139     IN      A       137.208.20.10

;; Query time: 2 msec
;; SERVER: 195.3.86.139#53(195.3.86.139)
;; WHEN: Mon May 13 16:22:11 2013
;; MSG SIZE  rcvd: 176
```

Nslookup:

```
root@webduxv91:~# nslookup www.wu-wien.ac.at
Server:         195.3.86.139
Address:        195.3.86.139#53

Non-authoritative answer:
Name:   www.wu-wien.ac.at
Address: 137.208.3.113
Name:   www.wu-wien.ac.at
Address: 137.208.3.114
Name:   www.wu-wien.ac.at
Address: 137.208.3.112
```

DNS - Resource Record

DNS speichert nicht nur die Domain-IP-Beziehung, sondern auch viele weitere Informationen. Diese kann man mithilfe des kleinsten Informationseinheit des DNS, dem Resource Record (RR), abgefragt werden.

Dieser hat folgende Struktur:

name [ttl] [class] type rdata
www 3600 IN A 137.208.3.82

name - Enthält den Host- oder Domainnamen
ttl - Anzahl in Sekunden, wie lange ein anderer Nameserver das Ergebnis zwischenspeichert
class -Protokollgruppe zu der RR gehört. IN (Internet).
type - Spezifiziert den RR-Typ (derzeit 25 Typen)
rdata - Daten die den RR näher beschreiben (IP Adresse, Mailexchanger, ...)

DNS - Typen

A	Host Adresse	**www IN A 137.208.3.82**
CNAME	Alias Name	**web IN CNAME www**
NS	Name Server	**@ IN NS ns1.wu-wien.ac.at**
MX	Mailexchanger	**@ IN MX 10 mx1.wu-wien.ac.at**
TXT	Zusätzliche Info, SPF, ...	**@ IN TXT "v=spf1 ip4:213.165.64.0/23 -all"**
SOA	Start of a Zone Authority	**@ IN SOA zns1.eunet.at. hostmaster.eunet-ag.at. 2003044845 3600 3600 604800 86400**
PTR	Pointer für Reverse DNS	**82 IN PTR www.wu-wien.ac.at**
AAAA	Ipv6	**cosi IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8**

DNS - Zone

Ein Standard Zonefile einer Domaine hat folgendes Aussehen:

```
$TTL 86400      ; 1 day
@                       IN SOA  zns1.eunet.at. hostmaster.eunet-ag.at. (
                                2003010201 ; serial
                                10800      ; refresh (3 hours)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                3600       ; negative (1 hour)
                                )
                        NS      zns1.eunet.at.
                        NS      zns2.eunet.at.
szojak.at.              600     IN      MX      10 mx.eunet.at.
szojak.at.              86400   IN      TXT     "v=spf1 ip4:193.154.160.0/24 -all"
www.szojak.at.          86400   IN      CNAME   vi13.eunet.at.
```

Default Time to live (TTL): Nach dieser Zeitspanne werden Einträge im Cache ausgetragen

Refresh: Diese gibt an, nach welcher Zeitdauer der Secondary Nameserver beim Primary Nameserver die Seriennummer und ggf. den neuen Datensatz für diese Zone holen soll.

Retry: Wenn der Secondary Nameserver den Primary Nameserver nicht erreichen konnte, versucht er nach der genannten Zeit erneut einen Verbindungsaufbau.

Expire: Nachdem die hier genannte Zeit verstrichen ist und der Secondary Nameserver den Primary Nameserver noch immer nicht erreicht hat, gibt er für diese Zone keine authoritativen Antworten mehr.

Negative: Gibt an, wie lange der fragende Nameserver eine Nicht- bzw. Falsch-Antwort speichern soll.

Die einzelnen Einträge werden durch Punkte voneinander getrennt. Ein Domainname wird mit einem Punkt abgeschlossen (Sollte dieser im Zonefile vergessen worden sein, so wird automatisch die Domaine angehängt!!!) Ein korrekter, vollständiger Domainname (auch Fully Qualified Domain-Name (FQDN) genannt) lautet etwa *www.wu-wien.ac.at.* .

Ein Domainname darf inklusive aller Punkte maximal 255 Zeichen lang sein und wird immer von rechts nach links delegiert und aufgelöst (siehe Beispiele am Ende).

Domainen sollten immer auf mindestens zwei DNS-Server delegiert werden, diese sollten aus Sicherheitsgründen nicht im selben Netzwerksegment stehen.

Änderungen in der Zone finden nur im ZoneFile am Primary DNS-Server statt, dieser schickt die Änderungen an den/die Secondary DNS-Server weiter (Zonetransfer).

Sicherheit

DNS-Spoofing bezeichnet einen Angriff, bei dem es einem Angreifer gelingt die Zuordnung zwischen einem URL und der zugehörigen IP-Adresse zu fälschen. Dies kann durch unterschiedliche Vorgehensweisen erreicht werden:

Cache Poisoning ist ein Internet-Angriff, bei dem ein Hacker in den Cache eines Nameservers gefälschte Daten einbringt. Ziel ist es, Clients, die unwissentlich auf diese gefälschten Daten zugreifen, auf manipulierte Webseiten zu lenken.

Durch **Manipulation der lokalen hosts-Datei** können trotz Eingabe der echten URL gefälschte IP-Adressen aufgelöst werden.

Abfragen einschränken, Nichtautorisierte Zonentransfers verhindern
chroot Umgebung

Transaction Signature – TSIG:

Ein DNS-Teilnehmer soll damit verifizieren können, dass der Partner, mit dem er kommuniziert auch tatsächlich der ist, der er vorgibt zu sein und dass empfangene DNS-Nachrichten auf dem Transportweg nicht verfälscht wurden. TSIG wird hauptsächlich bei der Server-Server-Kommunikation eingesetzt und weniger bei der Client-Server-Kommunikation.

Bei TSIG besitzen zwei oder mehr DNS-Server, die miteinander kommunizieren, den gleichen Schlüssel (symmetrischer Schlüssel), der manuell konfiguriert wird. Werden zwischen TSIG-Servern Daten ausgetauscht (z.B. beim Zonentransfer oder bei rekursiven Abfragen), so wird von jedem übertragenen DNS-Paket der MD5-Hash gebildet und in einem speziellen *TSIG Resource Record* angehängt. Der Empfänger führt mit seinem Schlüssel die

gleiche MD5-Operation durch und vergleicht die beiden Unterschriften. Sind sie identisch, so stammen die Daten vom gewünschten Partner und wurden nicht verfälscht.

Whois

Whois ist ein Suchdienst mit dem Informationen zu Internet-Domains, IP-Adressen und Handles, etc. abgefragt werden können.

Verwendet wird das Protokoll TCP auf Port 43.

```
whois wu-wien.ac.at@whois.nic.at

domain:         wu-wien.ac.at
registrant:     WVEU926708-NICAT
admin-c:        PM1430050-NICAT
tech-c:         AN1433912-NICAT
tech-c:         PM1430050-NICAT
nserver:        ns1.wu-wien.ac.at
remarks:        137.208.10.10
nserver:        ns2.wu-wien.ac.at
remarks:        137.208.20.10
nserver:        ns5.univie.ac.at
remarks:        193.171.255.77
changed:        20010823 16:56:09
source:         AT-DOM

personname:
organization:   WUnet Vienna Economic University Network
street address: Augasse 2-6
postal code:    A-1090
city:           Vienna
country:        Austria
e-mail:         postmaster@wu-wien.ac.at
nic-hdl:        WVEU926708-NICAT
changed:        20010823 16:56:09
source:         AT-DOM

personname:     Peter Mika
organization:
street address: Vienna Economic University
street address: Augasse 2-6
street address: A-1090 Wien
postal code:
city:
country:
phone:          +43 1 31336 4787
fax-no:         +43 1 31336 702
e-mail:         mika@wu-wien.ac.at
nic-hdl:        PM1430050-NICAT
changed:        20031129 02:55:19
source:         AT-DOM

personname:     Alfred Nagl
organization:
street address: Wirtschaftsuniversitaet Wien
street address: Augassse 2-6
street address: 1090 Wien
postal code:
city:
country:
phone:          +43 1 31336 4811
fax-no:         +43 1 31336 702
e-mail:         nagl@wu-wien.ac.at
nic-hdl:        AN1433912-NICAT
changed:        20031129 04:31:34
source:         AT-DOM
```

```
whois 137.208.3.82@whois.ripe.net

inetnum:      137.208.0.0 - 137.208.255.255
remarks:      **** INFORMATION FROM ARIN OBJECT ****
remarks:      netname: WU-WIEN
descr:        Wirtschaftsuniversitaet Wien
descr:        EDV Zentrum  Augasse 2-6Vienna
remarks:      country: AT
admin-c:      AN1100-RIPE
tech-c:       AN1100-RIPE
remarks:      changed: hostmaster@arin.net 19900103
remarks:      changed: hostmaster@arin.net 20010724
remarks:      **** INFORMATION FROM RIPE OBJECT ****
netname:      WU-WIEN
descr:        Wirtschaftsuniversitaet Wien, ZID
descr:        Augasse 2-6; A-1090 Wien; Austria
country:      AT
admin-c:      PM16-RIPE
tech-c:       AN50
mnt-by:       AS1776-MNT
status:       ASSIGNED PI
source:       RIPE # Filtered
```

```
person:       Peter Mika
address:      Vienna Economic University
address:      Augasse 2-6
address:      A-1090 Wien
phone:        +43 1 31336 4787
fax-no:       +43 1 31336 702
e-mail:       mika@wu-wien.ac.at
nic-hdl:      PM16-RIPE
mnt-by:       AS1776-MNT
source:       RIPE # Filtered

person:       Alfred Nagl
address:      Wirthschaftsuniversitaet Wien EDV-Zentrum
address:      Augasse 2-6Vienna
address:      AT
phone:        +1 1 31336 4811
e-mail:       nagl@wu-wien.ac.at
nic-hdl:      AN1100-RIPE
mnt-by:       RIPE-ERX-MNT
source:       RIPE # Filtered

person:       Alfred Nagl
address:      Wirtschaftsuniversitaet Wien
address:      Augassse 2-6
address:      1090 Wien
phone:        +43 1 31336 4811
fax-no:       +43 1 31336 702
e-mail:       nagl@wu-wien.ac.at
nic-hdl:      AN50
mnt-by:       ACONET-LIR-MNT
source:       RIPE # Filtered

% Information related to '137.208.0.0/16AS1776'

route:        137.208.0.0/16
descr:        WU-WIEN
origin:       AS1776
mnt-by:       AS1776-MNT
source:       RIPE # Filtered
```

Der administrative Ansprechpartner (**admin-c)** ist die Kontaktperson
Der technische Ansprechpartner (**tech-c**) betreut in technischer Hinsicht.

http://www.ripe.net
http://www.iana.org

Übungsbeispiele

Abfragen mit dig, nslookup, host und whois

IP-Adresse(n) von www.orf.at

MX-Eintrag von inode.at

SPF-Einträge von gmx.at

Whois für 193.154.160.60