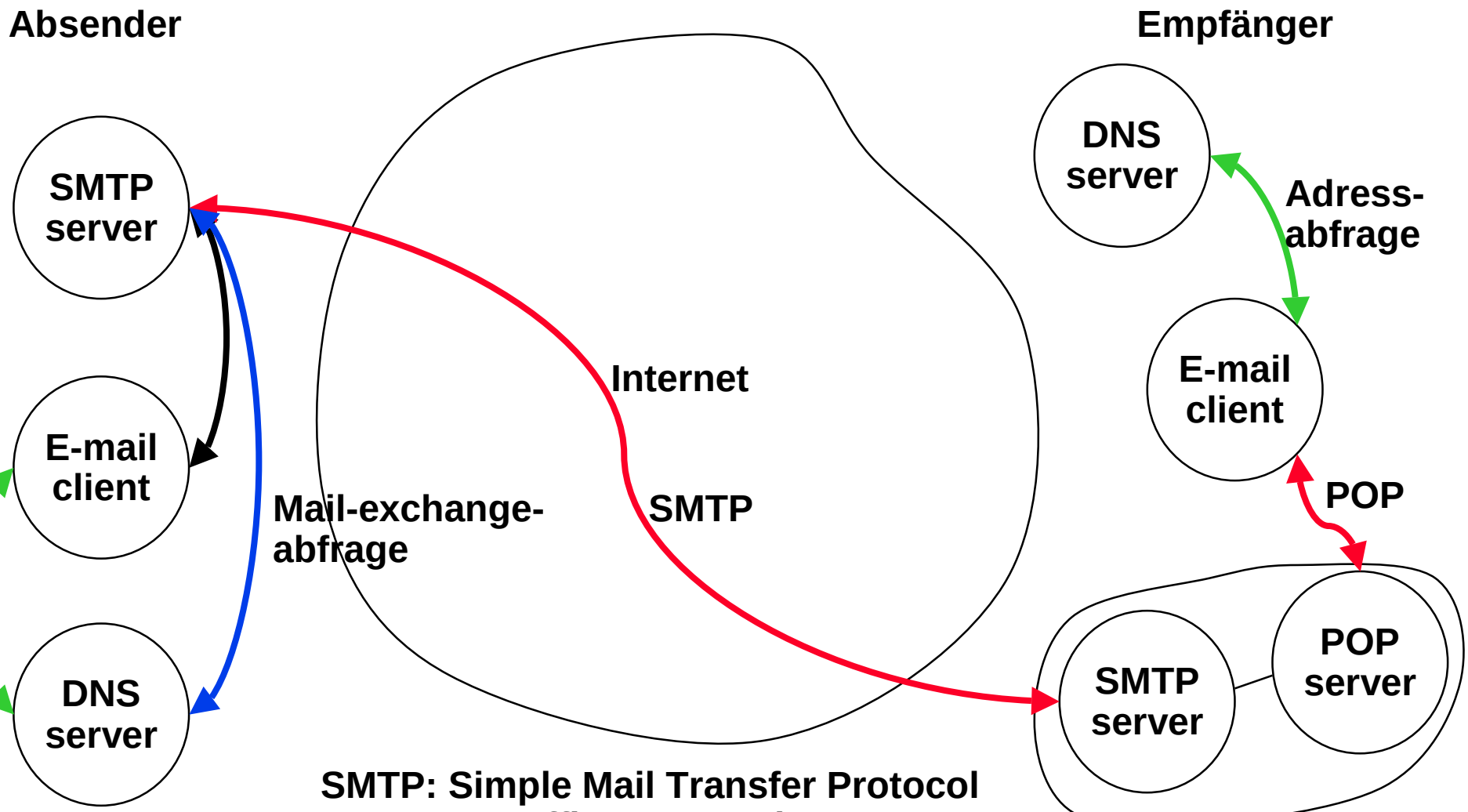
Namen und Adressen:
Das Domain Name System (DNS)
und seine Anwendung im E-mail-System des Internet

Motivation: E-mail-Infrastruktur des Internet



SMTP: Simple Mail Transfer Protocol
POP: Post Office Protocol

Ziele des "Domain Name System"

- Auf Ebene der Transportschicht wird das Tupel (IP-Adresse, Port-Nummer) als Endpunkt einer Kommunikationbeziehung (z.B. einer Verbindung) verwendet.
- Adressen sind unhandlich und schlecht merkbar.
- Adressen sind änderungsanfällig (z.B. wenn ein Server an ein anderes Subnetz angeschlossen wird).
- Wir wünschen Namen als Bezeichner von Objekten (Hosts, elektronische Briefkästen).
- Das *Domain Name System (DNS)* erlaubt eine benutzerfreundliche Benennung von Objekten im Internet und versteckt Adressänderungen.

Vergabe von Namen (Namensautorität)

- Der Namensraum ist hierarchich und hat die Form eines beliebig tiefen Baumes.
- Jeder Knoten (Organisation) ist verantwortlich für seinen Unterbaum. -> Vergibt unmmittelbar untergeordnete Namen.
- Die Namensstruktur ist eine logische Struktur und muss nicht der Netztopologie entsprechen.
- Die Verschachtelung kann beliebig tief sein, also z.B.

  Rechner.Universität.Land

  oder

  Rechner.Institut.Abteilung.Universität.Land

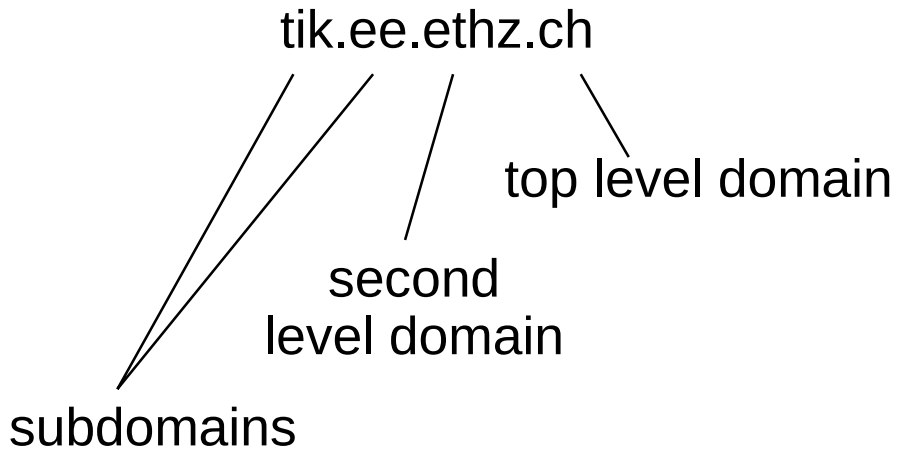
Domain Namen im Internet

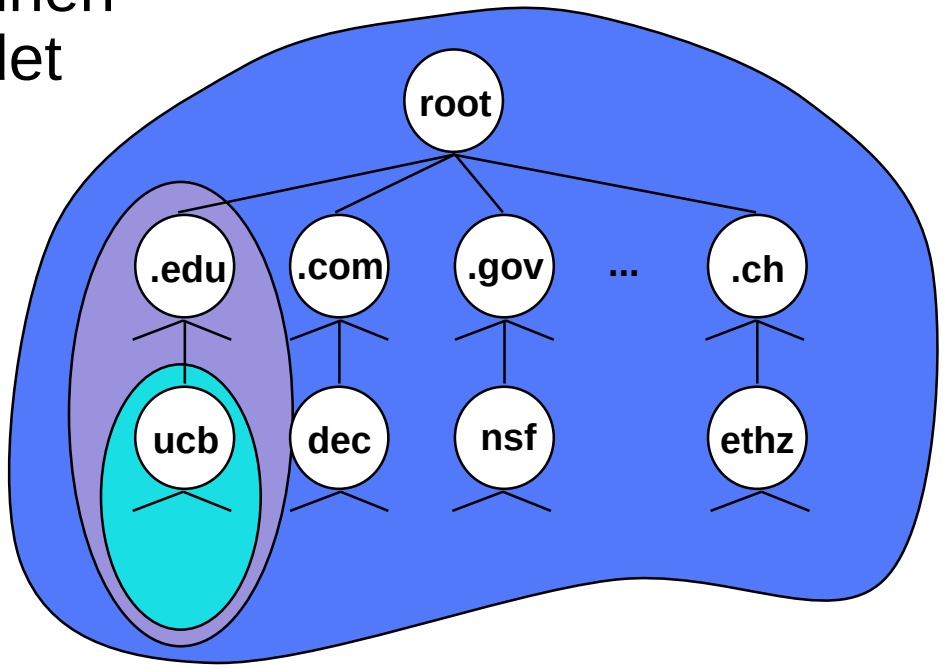
- DNS definiert Syntax und Regeln für das Delegieren der Namens-autorität sowie die Implementierung eines verteilten Systems zur Abbildung von Namen auf Adressen.
- Domain Namen haben die Form "Subdomain.Subdomain.Domain", also z.B. "komsys.tik.ethz.ch", wobei die hierarchisch höchst-liegende Domain ganz rechts steht (Ausnahme: Grossbritannien).
- Gültige "top level" Domain Namen sind:

COM	Kommerzielle Organisationen
EDU	Ausbildungseinrichtungen, Universitäten usw.
GOV	Staatliche Organisationen
MIL	Militärische Einrichtungen
NET	Grosse Netzwerkbetreiber
ORG	Andere, vor allem nichtkommerzielle, Organisationen
ARPA	Ursprüngliche Internet "top level" Domain, heute kaum noch verwendet
INT	Internationale Organisationen
cc	2-buchstabiger Landescode nach ISO 3166 (für die Schweiz z.B. "CH")
biz, museum, info, …	neue TLD

Benennbare Objekte, Syntax und Abbildung auf Adressen

- DNS-Namen können auf verschiedenartige Objekte abgebildet werden, z.B Rechneradressen, e-Mail-Adressen usw.
- Ein Eintrag "dn1.ethz.ch" kann also einen einzelnen Rechner bezeichnen, und ”inf.ethz.ch" ein e-Mail-Domain. Dem Namen sieht man diesen Unterschied nicht an.
- Verschiedene DNS-Namen können auf das gleiche Objekt abgebildet werden (alias).





Administration des Namensraums und Betrieb des DNS

- Zone: Unterbaum des Namensraums, der als Einheit verwaltet wird, z.B. ein second-level domain wie *ethz.ch.*
- Zonen können in untergeordnete Zonen aufgeteilt werden.
- Ein *primary name server* ist für eine oder mehrere Zonen zuständig. Primary name servers werden aus einer Datenbank (Textfile) geladen.
- Einer oder mehrere redundante *secondary name servers* erhöhen die Verfügbarkeit . Secondary name servers werden vom primary geladen (zone transfer).
- Secondary name servers sind für Betreiber von Zonen obligatorisch
- *root server* binden die oberste Ebene des DNS zusammen. Jeder name server muss die IP-Adressen der root server kennen.

Liste der root servers

```
/netinfo/root-servers.txt                    Sep 97
The following hosts are functioning as root domain name servers
for the Internet:

HOSTNAME                NET ADDRESSES      SERVER PROGRAM

A.ROOT-SERVERS.NET   198.41.0.4           BIND (UNIX)
B.ROOT-SERVERS.NET   128.9.0.107          BIND (UNIX)
C.ROOT-SERVERS.NET   192.33.4.12          BIND (UNIX)
D.ROOT-SERVERS.NET   128.8.10.90          BIND (UNIX)
E.ROOT-SERVERS.NET   192.203.230.10       BIND (UNIX)
F.ROOT-SERVERS.NET   192.5.5.241          BIND (UNIX)
G.ROOT-SERVERS.NET   192.112.36.4         BIND (UNIX)
H.ROOT-SERVERS.NET   128.63.2.53          BIND (UNIX)
I.ROOT-SERVERS.NET   192.36.148.17        BIND (UNIX)
J.ROOT-SERVERS.NET   198.41.0.10          BIND (UNIX)
K.ROOT-SERVERS.NET   193.0.14.129         BIND (UNIX)
L.ROOT-SERVERS.NET   198.32.64.12         BIND (UNIX)
M.ROOT-SERVERS.NET   202.12.27.33         BIND (UNIX)
```

Namensauflösung

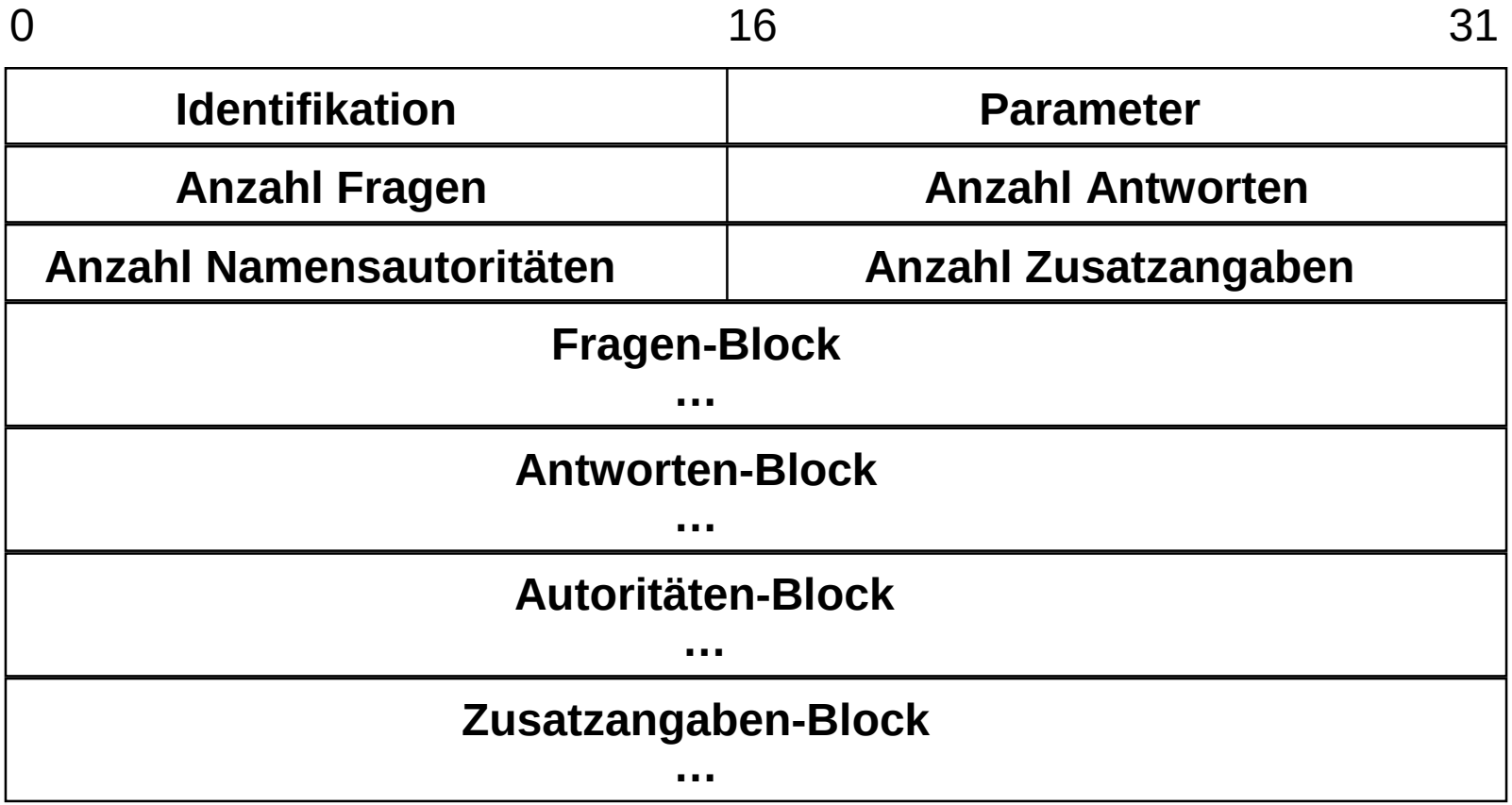
- Die Namensauflösung wird logisch immer an der Wurzel des Baums gestartet, und arbeitet dann "abwärts”.
- Die Namensauflösung wird durch einen DNS Client (DNS resolver), der in die Applikation eingebunden ist, initiiert.
- Abfragen
  - gezielt an einzelne name server
  - *rekursiv* an das ganze DNS
- Erhält ein Namens-Server eine Anfrage, prüft er, ob der Name in seinem eigenen Unterbaum liegt. Wenn ja, kann er die Anfrage beantworten, sonst kann er die Abfrage an den nächsthöheren Server oder einen root server weiterleiten.
- Ein Abfrage-Klient (resolver) muss also nur die Adresse eines (bzw. "seines") Namens-Servers kennen (/etc/resolv.conf).

Ausnutzung der Lokalität von Abfragen

- Da die meisten Abfragen lokal sind werden in der Realität viele Abfragen lokal beantwortet (bottom up).
- DNS Server führen einen Cache für kürzlich verwendete Abfragen.
- Antworten aus einem Cache sind *non-authoritative*.
- Antworten von einem primary oder secondary server sind *authoritative*.

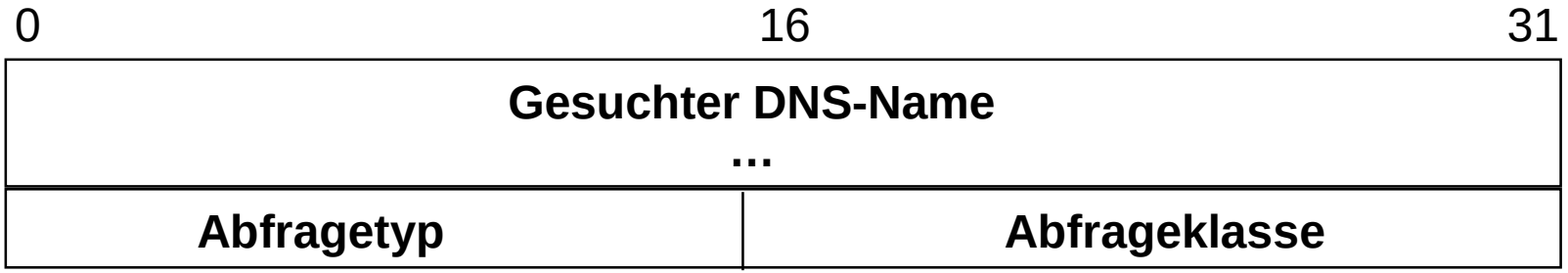
Format von DNS Meldungen I

Für Abfragen und Antworten wird dasselbe Format verwendet:

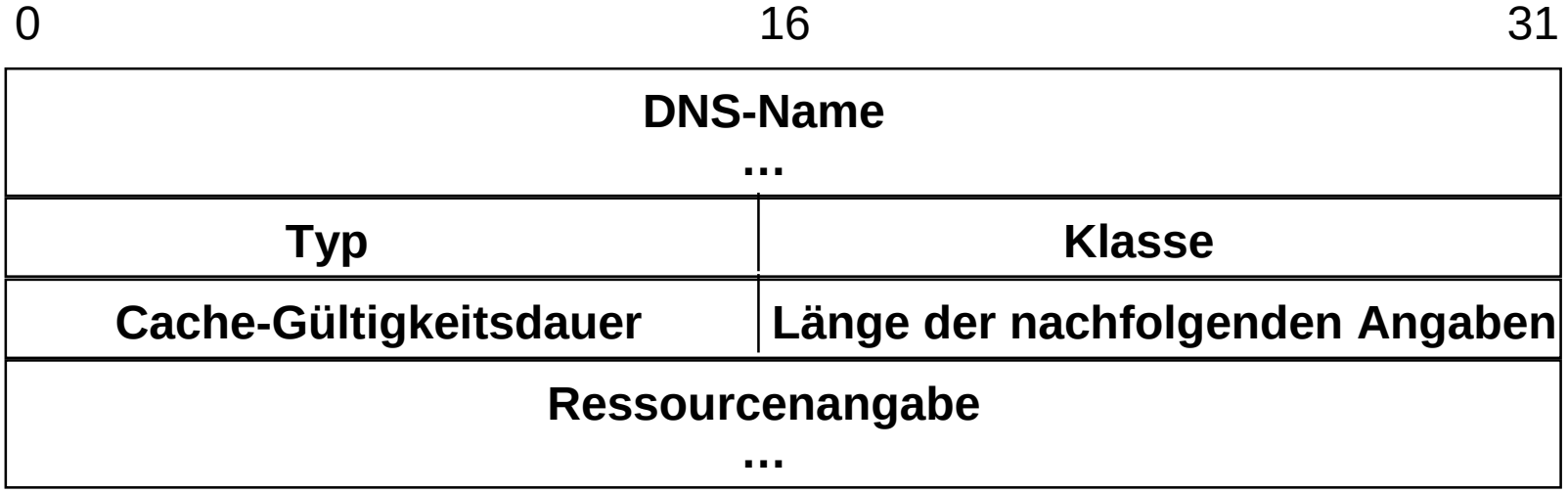


Format von DNS Meldungen II

DNS Query - Fragenblock



DNS Response - Antwortenblock



Format des Parameter-Felds

0	Operation 0 Abfrage 1 Antwort
1-4	Abfragetyp 0 Standard 1 Inverse 2 Server-Statusabfrage 3 unbenutzt
5	Gesetzt, wenn Antwort garantiert (Server ist für den Domain zuständig)
6	Gesetzt, wenn Antwort auf 512 Bytes verkürzt
7	Gesetzt, wenn rekursive Bearbeitung erwünscht (sonst: iterativ)
8	Gesetzt, wenn rekursive Bearbeitung möglich
9-11	Reserviert (0)
12-15	Antworttyp 0 Kein Fehler 1 Formatfehler in der Abfrage 2 Fehler des Servers 3 Name existiert nicht

Komprimieren von Domain Namen und Antworten

- Domainnamen in der Antwort werden als Sequenz von Marken repräsentiert. Jedes Label beginnt mit einer Längenangabe, gefolgt von einer Zeichenfolge (Domainname). Da in einer Antwort mehrere Einzelantworten beantwortet werden können, wird jede Zeichenfolge nur einmal gespeichert, bei mehrfacher Verwendung steht dann statt der Längenangabe und der Zeichenfolge ein Zeiger auf die Namensinformation in einer anderen Antwort in der Marke.
- Der Systemadministrator kann Domain-Ergänzungen definieren, die bei unvollständiger Namensangabe automatisch "ausprobiert" werden, z.B.:

  .komsys.tik.ethz.ch
  .tik.ethz.ch
  null

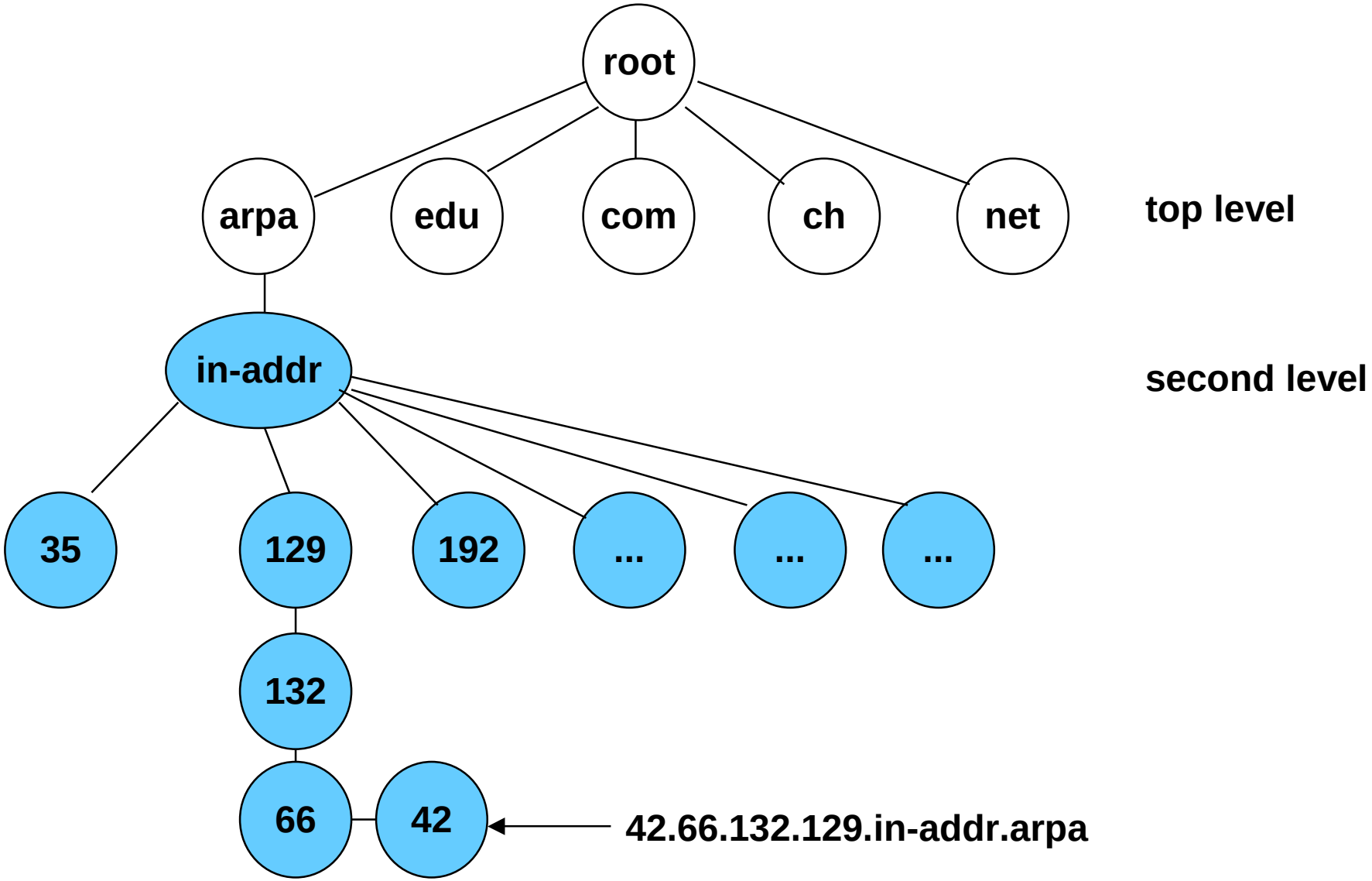
  .systech.tik.ethz.ch
  .ethz.ch

- Vollständige Namen: “.” am Ende, z.B. www.ethz.ch.

Inverse Abfragen ("Pointer-Abfragen”)

- Inverse Abfrage: Gegeben ist eine IP-Adresse, gesucht die dazugehörigen Domainnamen.
- Oft sind inverse Abfragen erforderlich, z.B. bei der “Authentisierung” von IP-Adressen.
  - Rlogin basiert seine Autorisierung auf eine Liste von zugelassenen Domainnamen.
- Problem: Der DNS-Namensraum ist nach der Namenshierarchie organisiert. Die Suche nach einer IP-Adresse würde das Durchsuchen des ganzen DNS erfordern.
- Spezieller second level domain “in-addr.arpa.” enthält eine nach IP-Adressen organisierte Hierarchie.
- “in-addr.arpa.” ist somit ein Index für die Suche nach IP-Adressen.

Namensraum für inverse Abfragen



Objekttypen in DNS

Typ	Bezeichnung	Inhalt
A	Hostadresse	32-Bit IP-Adresse
CNAME	Kanonischer Name	Domainname für ein Alias
HINFO	CPU und Betriebssystem	Informationen über den Host
MINFO	E-Mail Information	Informationen über Mailbox
MX	E-Mail Exchanger	16-Bit Präferenz und Name des Host, der für diese Domain als Mail-Server fungiert
N	Namens-Server	Name des verbindlichen Servers für diese Domain
PTR	"Pointer"	Domainname
SOA	Namensautorität	Mehrere Felder, die angeben, für welche Teile der Namenshierarchie der Server zuständig ist
TXT	Beliebiger Text	Nicht interpretierte ASCII-Zusatzinformation

nslookup - UI für DNS

```
#pragma ident   "@(#)nslookup.help      1.6     96/09/12 SMI"

Commands:       (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands; see nslookup(1) for details
set OPTION      - set an option
    all         - print options, current server and host
    [no]debug   - print debugging information
    [no]d2      - print exhaustive debugging information
    [no]defname - append domain name to each query
    [no]recurse - ask for recursive answer to query
    [no]vc      - always use a virtual circuit
    domain=NAME - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME   - set root server to NAME
    retry=X     - set number of retries to X
    timeout=X   - set initial time-out interval to X seconds
    querytype=X - set query type, e.g., A,ANY,CNAME,HINFO,MX,PX,NS,PTR,SOA,TXT,WKS
    port=X      - set port number to send query on
    type=X      - synonym for querytype
    class=X     - set query class to one of IN (Internet), CHAOS, HESIOD or ANY
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional USER at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -h          -  list HINFO (CPU type and operating system)
    -s          -  list well-known services
    -d          -  list all records
    -t TYPE     -  list records of the given type (e.g., A,CNAME,MX, etc.)
view FILE       - sort an 'ls' output file and view it with more
exit            - exit the program, ^D also exits
```

Einige DNS-Abfragen mit nslookup

```
> set querytype=a
> www.ethz.ch
Server:  dns2.ethz.ch
Address:  129.132.250.220

Name:    w3.ethz.ch
Address:  129.132.200.35
Aliases:  www.ethz.ch

> set querytype=mx
> ethz.ch
Server:  dns2.ethz.ch
Address:  129.132.250.220

ethz.ch preference = 10, mail exchanger = bernina.ethz.ch
ethz.ch nameserver = dns1.ethz.ch
ethz.ch nameserver = dns2.ethz.ch
ethz.ch nameserver = dns3.ethz.ch
bernina.ethz.ch internet address = 129.132.1.11
bernina.ethz.ch internet address = 129.132.98.11
dns1.ethz.ch    internet address = 129.132.98.12
(…)
> www.ethz.ch
Server:  dns2.ethz.ch
Address:  129.132.250.220

www.ethz.ch     canonical name = w3.ethz.ch
ethz.ch
        origin = baloo.ethz.ch
        mail addr = brunner@kom.id.ethz.ch
        serial = 1999062514
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        minimum ttl = 86400 (1 day)
```

```
> ee.ethz.ch
Server:  dns2.ethz.ch
Address:  129.132.250.220

ee.ethz.ch      preference = 10, mail exchanger = ee00.ethz.ch
ee.ethz.ch      preference = 20, mail exchanger =
bernina.ethz.ch
ethz.ch nameserver = dns1.ethz.ch
ethz.ch nameserver = dns2.ethz.ch
ethz.ch nameserver = dns3.ethz.ch
ee00.ethz.ch    internet address = 129.132.98.179
bernina.ethz.ch internet address = 129.132.98.11
(…)
> tik.ee.ethz.ch
Server:  dns2.ethz.ch
Address:  129.132.250.220

tik.ee.ethz.ch  preference = 20, mail exchanger =
bernina.ethz.ch
tik.ee.ethz.ch  preference = 10, mail exchanger = tik2.ethz.ch
ethz.ch nameserver = dns1.ethz.ch
ethz.ch nameserver = dns2.ethz.ch
ethz.ch nameserver = dns3.ethz.ch
bernina.ethz.ch internet address = 129.132.1.11
tik2.ethz.ch    internet address = 129.132.119.132
(…)
> set querytype=ptr
> 129.132.0.0
Server:  dns2.ethz.ch
Address:  129.132.250.220

0.0.132.129.in-addr.arpa        name = eth-net.ethz.ch
132.129.in-addr.arpa    nameserver = bernina.ethz.ch
132.129.in-addr.arpa    nameserver = dns1.ethz.ch
bernina.ethz.ch internet address = 129.132.98.11
dns1.ethz.ch    internet address = 129.132.98.12
```

Bemerkungen zum DNS

- Das DNS ist ein eher statischer Verzeichnisdienst
- Nicht geeignet für dynamische Abbildung; z.B. können Hosts, denen eine IP-Adresse dynamisch zugeordnet wird, nicht unterstützt werden.
- Eignet sich nicht für die Speicherung von benutzerbezogenen Daten - kein Benutzerverzeichnis.
- Normierung für ein etwas dynamischeres DNS ist im Gang. (http://www.ietf.org/html.charters/dnsind-charter.html)
- Erweiterungen für die Unterstützung der langen Adressen von IPv6 (128 Bit) sind definiert. (name server cb4.ethz.ch)

```
Server:  cb4-e.ethz.ch
Address:  129.132.66.58

cb2.ipv6.tik.ee.ethz.ch canonical name = crossbow2.ipv6.tik.ee.ethz.ch
crossbow2.ipv6.tik.ee.ethz.ch   IPv6 address = 3ffe:2000:400:1:260:8ff:fe36:1ce3
crossbow4.ipv6.tik.ee.ethz.ch   IPv6 address = 3ffe:2000:400:1:260:8ff:fe36:1d09
crossbow4.ipv6.tik.ee.ethz.ch   internet address = 129.132.66.58
```

Weiterführende Literatur

- RFC 1035: Mockapetris, P.V., "Domain names - implementation and specification", November 1987
- RFC 1034: Mockapetris, P.V., "Domain names - concepts and facilities", November 1987
- RFC 1033: Lottor, M., "Domain administrators operations guide, November 1987
- RFC 1032: Stahl, M.K. "Domain administrators guide", November 1987
- RFC 920: Postel, J.B.; Reynolds, J.K., "Domain requirements", October 1984
- Sun Microsystems "Network and Communications Administration Handbook" (Dokumentation zu SunOS/SOLARIS-Betriebssystem)
- "man" nslookup, resolver, resolve.conf, named