

DNS-(Domain Name Service): „Frag doch den, der zuständig ist!“

Neulich im Internet-Cafe: Wann haben wir eigentlich wieder Berufsschule? Das müsste doch eigentlich auf der Homepage unserer Berufsschule stehen. Web-Browser gestartet und <http://www.bsinfo.eu> eingegeben. Super, nächste Woche ist Unterricht!

Aber Moment mal, woher weiß eigentlich der Computer im Internet Cafe die IP-Adresse unserer Schule? Das macht doch der DNS-Abfragemechanismus, oder ...

Im Prinzip ist das Domain Name System eine riesige verteilte Datenbank, die den benutzerfreundlichen, sprechenden und leicht zu merkenden Rechnernamen die passenden numerischen IP-Adressen zuordnet. Die einzelnen Elemente sind dabei über Tausende von Rechnern (*Nameserver*) verteilt, die jeweils Informationen für einen speziellen Zweig des Internets bereithalten. An der Wurzel des hierarchischen Baumes stehen zurzeit 13 Root-Nameserver, die die Informationen über alle Top Level Domains (TLD) enthalten. Die TLD werden von der ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet.



Quelle: <https://www.sdsc.edu/News%20Items/PR012303.html> abgerufen 25.4.2020

- Es gibt 13 Root-Nameserver (A.ROOT-SERVER - M-ROOT-SERVER)
- Im *Root-Zonen-File* des A.ROOT-SERVERs werden Informationen (über die darunter liegenden Top –Level-Domains TLD) zentral verwaltet. <https://root-servers.org/>
- Auf den Root-Servern B bis M befindet sich eine Kopie des *Root-Zonen-Files*.
- Jeder Nameserver kennt alle 13 Root-Nameserver.
- **Der Abfragen und Antworten laufen über Port 53 mit UDP oder TCP**

Ser-ver-na me	Betreiber	URL des Betreibers	IP v4 des Nameservers	IPv6-Adresse des Nameservers	Standort
A	Network Solutions	www.netsol.com	198.41.0.4	2001:503:ba3e::2:30	Herndon, VA, USA
B	Information Sciences Institute, USC	http://www.isi.edu/	128.9.0.107	2001:500:200::b	Marina Del Rey, CA, USA
C	PSINet	http://www.psi.net/	192.33.4.12	2001:500:2::c	Herndon, VA, USA
D	University of Maryland	http://www.umd.edu/	128.8.10.90	2001:500:2d::d	College Park, MD, USA
E	NASA	http://www.nasa.gov/	192.203.230.10	2001:500:a8::e	Mountain View, CA, USA
F	Internet Software Consortium	http://www.isc.org/	192.5.5.241	2001:500:2f::f	Palo Alto, CA, USA
G	Defense Information Systems Agency	http://nic.mil/	192.112.36.4	2001:500:12::d0d	Vienna, VA, USA
H	Army Research Laboratory	http://www.arl.mil/	128.63.2.53	2001:500:1::53	Aberdeen, MD, USA
I	NORDUNet	http://www.nordu.net/	192.36.148.17	2001:7fe::53	Stockholm, Schweden
J	TBD		198.41.0.10	2001:503:c27::2:30	Herndon, VA, USA
K	RIPE-NCC	http://www.ripe.net/	193.0.14.129	2001:7fd::1	London, Großbritannien
L	TBD		198.32.64.12	2001:500:9f::42	Marina Del Rey, CA, USA
M	WIDE	http://www.wide.ad.jp/	202.12.27.33	2001:dc3::35	Tokio, Japan

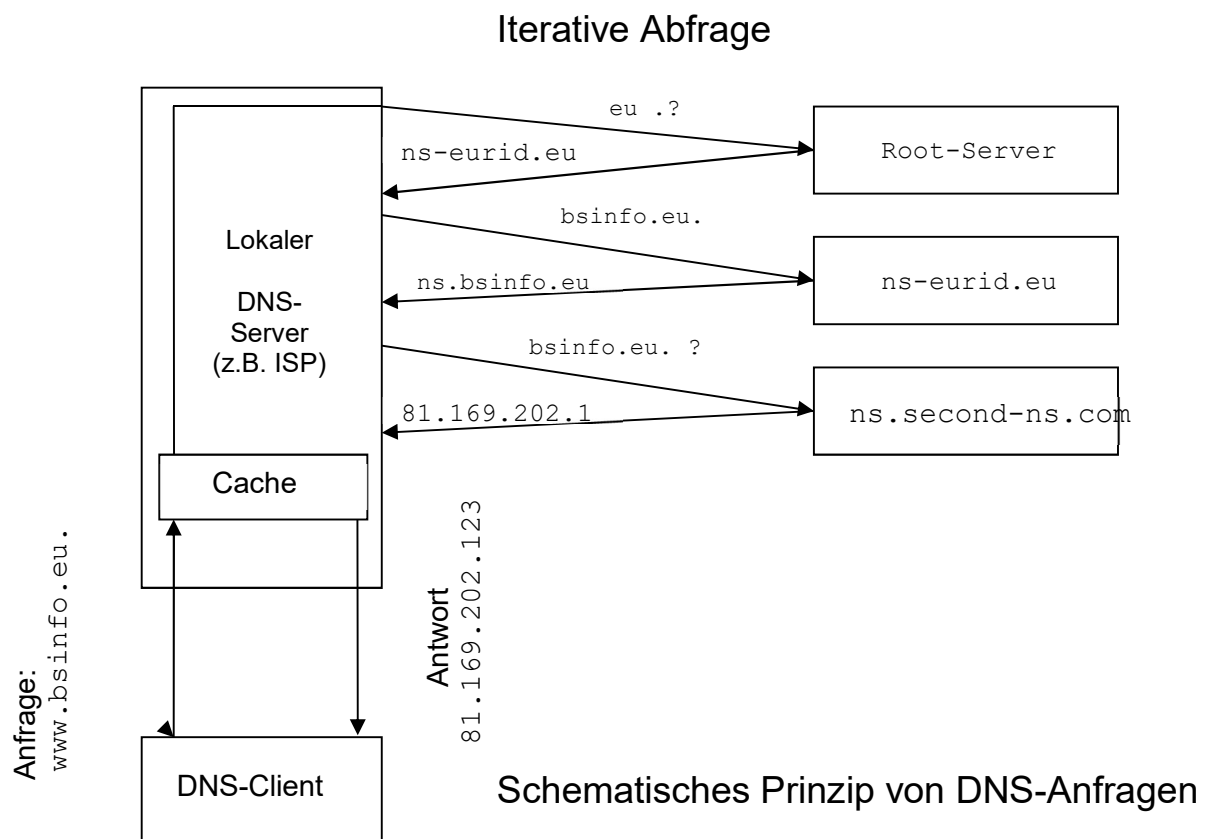
Für jede TLD sind dort die autoritativen Nameserver bekannt, die ihrerseits die lokalen Nameserver für die Second Level Domains ihrer TLD kennen müssen. So wissen die Root-Nameserver, dass für die TLD „de“ der Nameserver des DENIC (Deutsches Network Information Center) zuständig ist. Dieser wiederum weiß, dass für Informationen über Rechner in der Domain `bsinfo.eu` die betriebenen Nameserver zu befragen sind.

Das Grundprinzip des DNS ist die verteilte bzw. delegierte Zuständigkeit – jeder Nameserver besitzt die Autorität für eine bestimmte Zone des Namensraumes.

Das Prinzip, nach dem DNS-Anfragen beantwortet werden, könnte man salopp mit einem Satz beschreiben: „Frag doch denjenigen, der zuständig ist“. Die Kernaufgabe besteht demzufolge darin, denjenigen zu finden, der zuständig ist und autoritativ(aufgrund seiner Stellung zuständige) Auskunft geben kann. Dies erfolgt durch iterative (schrittweise annähernde) Befragung der übergeordneten Nameserver.

Ein Ziel dabei ist die möglichst dezentrale Auskunft um Zeit und Traffic zu sparen. Deshalb werden auch zuerst die Caches der lokalen Maschinen befragt und dann erst die übergeordneten DNS Server. Zuerst betrachten wir den Vorgang ohne Einbeziehung der Caches, wie er bei einer erstmaligen Abfrage abläuft. Damit also Ihr PC herausfinden kann, wie er den Web-Server der BS Informationstechnik www.bsinfo.eu erreicht, beauftragt er seinen lokalen Nameserver (zumeist des ISPs) mit einer entsprechenden Recherche. Dieser muss zunächst bei einem der Root-Nameserver anfragen, welcher Nameserver für die oberste Ebene (TLD) **eu**. zuständig ist, das ist **EURid (European Registry of Internet Domain Names)**, <https://eu-rid.eu/de/> ; [für de. ist es (de → dns.denic.de)], dort kann man mit <https://whois.eu-rid.eu/de/search/?domain=bsinfo.eu> erfragen wer den Namen registriert hat. In unserem Fall ist es die Vatron Rechenzentrum AG, unser Hoster(Registrar) unseres Webserver. <https://website.informer.com/bsinfo.eu> zeigt noch weitere Informationen, Stratos AG als Hoster IP 81.169.202.123 und DNS Server welche zuständig(authorisiert) sind: ns.second-ns.com , ns1.your-server.de, ns3.second-ns.de

Diesen wiederum muss er nach der Zuständigkeit für bsinfo.eu. befragen (→ns.second-ns.com). Im dritten Schritt erfolgt die Frage nach der Zuständigkeit für bsinfo.eu. Da ns.second-ns.com auch die Autorität (Zuständigkeit) für bsinfo.eu besitzt, kann er die IP-Adresse für bsinfo.eu selbst an den anfragenden lokalen DNS-Server im Internet-Cafe ausliefern, und dieser teilt seinem Client nun mit, welchen Computer er kontaktieren muss, um die gewünschten Informationen anzeigen zu können.



Neben dem Mechanismus der iterativen Abfrage gibt es auch die Möglichkeit, dass DNS-Server, falls sie eine Anfrage nicht beantworten können, diese an den übergeordneten DNS-Server (z.B. den des Providers) weiterleiten. Wir erinnern uns die dezentrale Auskunft ist ein Ziel (s.o). Die folgenden Blätter dienen zur Veranschaulichung wichtiger DNS-Begriffe.

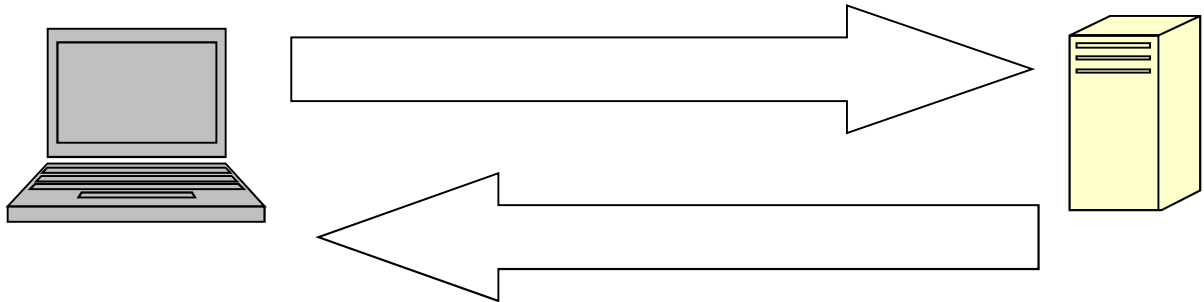
/

\

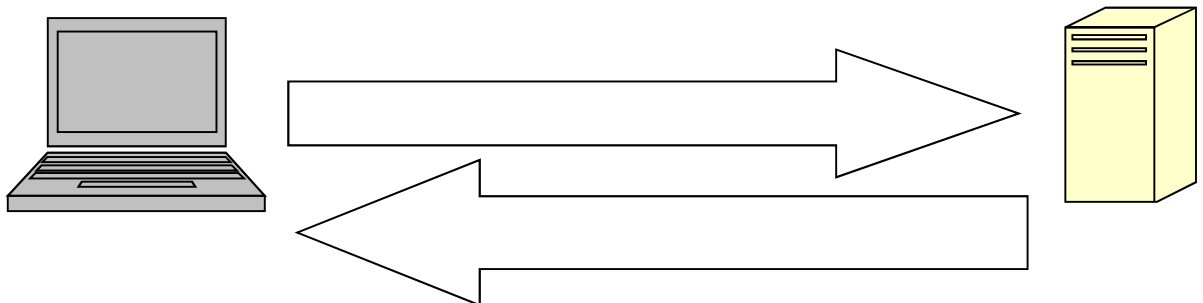


Merke: Das primäre DNS-Suffix gibt an,

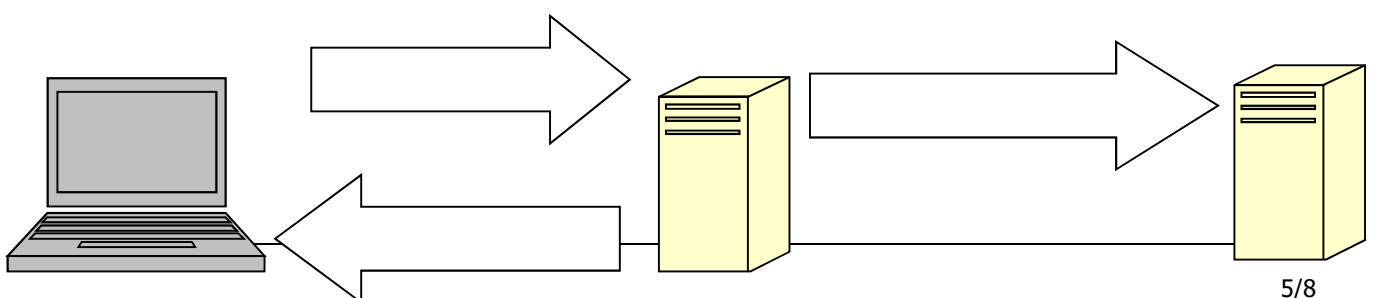
Forward-Lookup-Abfrage:



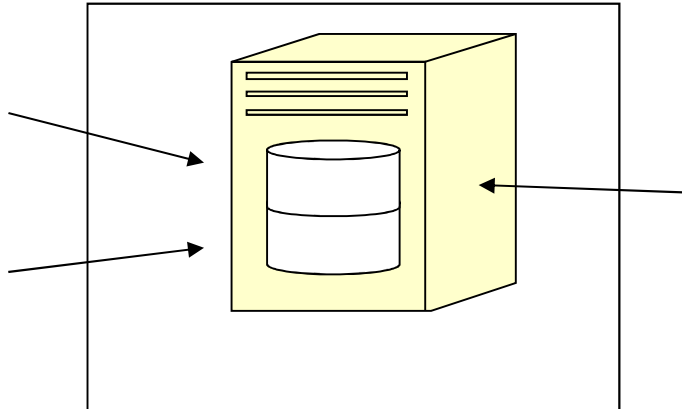
Reverse-Lookup-Abfrage:



Dynamisches DNS: Der DNS-Server erhält auch IP-Informationen vom DHCP-Server



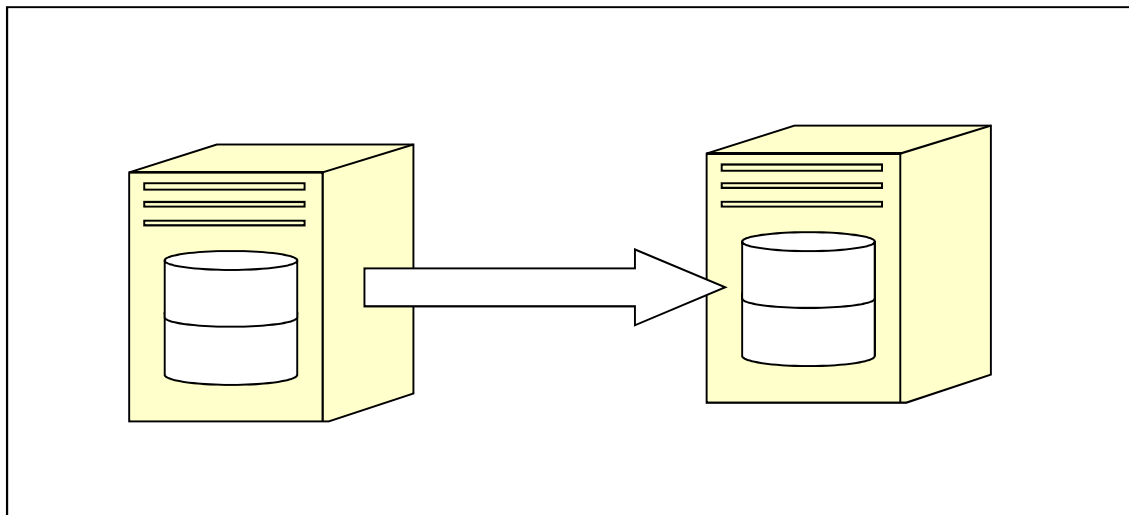
Begriff Zone:



Siehe: windows, system32, DNS

Begriff: Zonenübertragung

Zone: idealtec.intern



Bei der Zonenübertragung (-transfer) wird die DNS-Datenbank vom primären DNS-Server zum sekundären DNS-Server kopiert (=Single-Master-Replikation). Die DNS-Einträge können nur vom 1.DNS-Server (=Master-DNS-Srv) aktualisiert werden. Die Zonenübertragung findet innerhalb einer Zone statt.

Vorteile der Zonenübertragung:

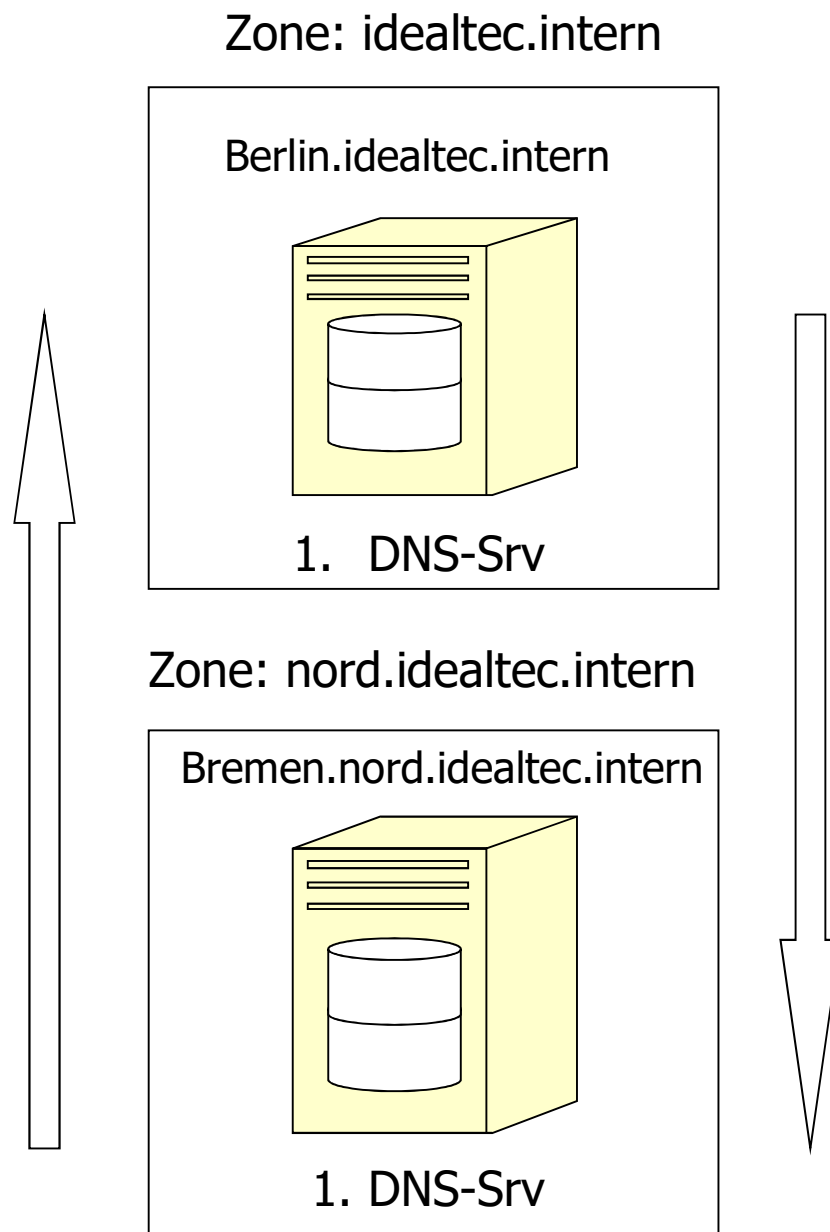
-

-
-

Begriff: Zonendelegierung und Weiterleitung

Zonendelegierung „läuft“ im DNS-Namensraum von oben nach unten und findet zwischen zwei Zonen statt. Die

Weiterleitung „läuft“ von unten nach oben.



Vorteile der Zonendelegierung:

-
-

Achtung: keine Ausfallsicherheit, Ausfallsicherheit entsteht nur durch Zonenübertragung!