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

Neulich im Internet-Cafe: Wann haben wir eigentlich wieder Berufsschule? Das müsste doch 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 des Webservers unserer Schule?
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 Domain Name Systems 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: Root Server Map - https://root-servers.org

- Im r*oot zone file* werden Informationen über die darunter liegenden Top –Level-Domains (TLD) zentral von der Firma Verisign verwaltet, die im Auftrag der IANA das r*oot zone file* verwaltet, signiert und für die Verteilung an die verschiedenen *root server operators* sorgt.
- Informationen über die Root-Nameserver sind in der root-hints (named.cache) Datei gespeichert.
- Jeder Nameserver kennt alle 13 Root-Nameserver.

HOSTNAME	IPv4 ADDRESSES	IPv6 ADDRESSES	OPERATOR / ORGANISATION
a.root-servers.net	*198.41.0.4*	*2001:503:ba3e::2:30*	*Verisign, Inc.*
b.root-servers.net	*199.9.14.201*	*2001:500:200::b*	*University of Southern California*
c.root-servers.net	*192.33.4.12*	*2001:500:2::c*	*Cogent Communications*
d.root-servers.net	*199.7.91.13*	*2001:500:2d::d*	*University of Maryland*
e.root-servers.net	*192.203.230.10*	*2001:500:a8::e*	*NASA (Ames Research Center)*
f.root-servers.net	*192.5.5.241*	*2001:500:2f::f*	*Internet Systems Consortium, Inc.*
g.root-servers.net	*192.112.36.4*	*2001:500:12::d0d*	*US Department of Defense (NIC)*
h.root-servers.net	*198.97.190.53*	*2001:500:1::53*	*US Army (Research Lab)*
i.root-servers.net	*192.36.148.17*	*2001:7fe::53*	*Netnod*
j.root-servers.net	*192.58.128.30*	*2001:503:c27::2:30*	*Verisign, Inc.*
k.root-servers.net	*193.0.14.129*	*2001:7fd::1*	*RIPE NCC*
l.root-servers.net	*199.7.83.42*	*2001:500:9f::42*	*ICANN*
m.root-servers.net	*202.12.27.33*	*2001:dc3::35*	*WIDE Project*

Recherchieren Sie im Internet (https://root-servers.org)!
a) Wie viele Instanzen der DNS Root-Server werden von den zwölf Organisationen aktuell betrieben!
- Stand (Datum): _____ - Anzahl: _____

b) Wie viele Instanzen werden aktuell alleine in Deutschland betrieben? - Anzahl: ____ (-> interaktive Karte!)

c) Wie heißen die beiden aktuell München am nächsten gelegenen Instanzen (-> interaktive Karte!)?
1. _____ 2. _____

Erklären Sie in diesem Zusammenhang den Begriff der Instanz!

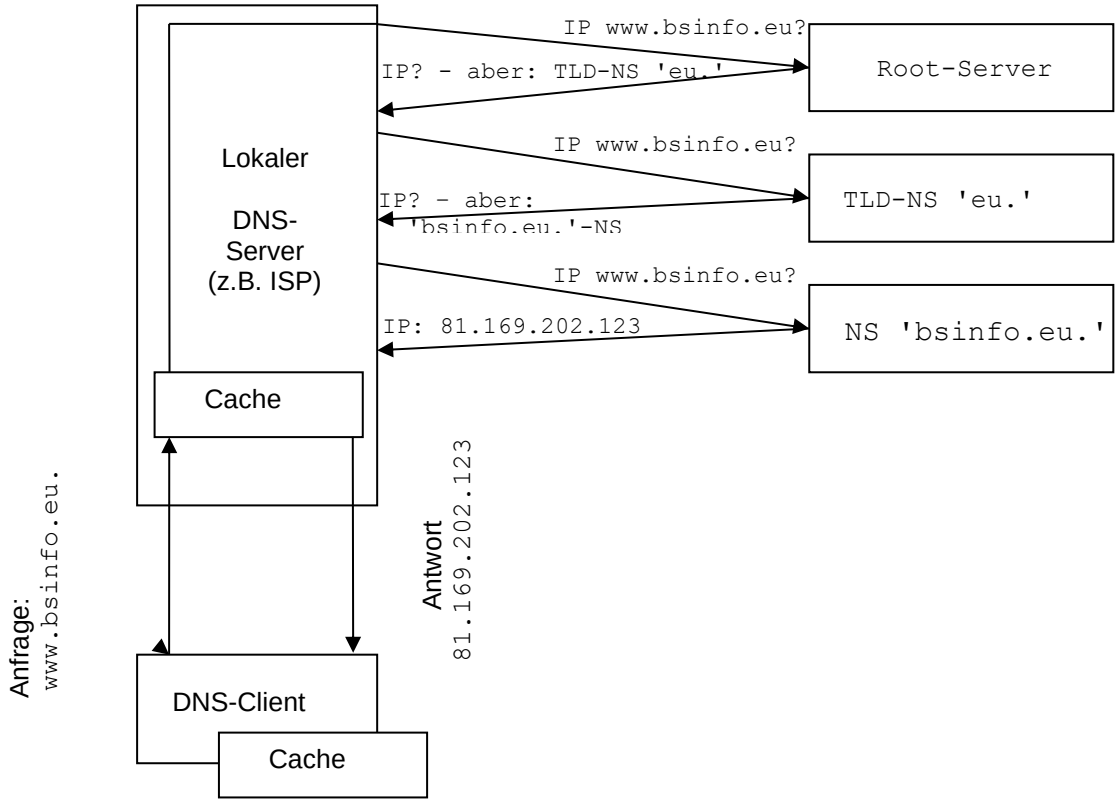
Instanz: _____

Jedem Root-Server sind für jede TLD 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 „eu.“ die Nameserver der EURid (European Registry of Internet Domain Names) in Belgien zuständig sind. Diese wiederum wissen, 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 DNS-Server zu finden, der zuständig ist und autoritativ (aufgrund seiner Stellung) Auskunft geben kann. Dies erfolgt durch iterative (schrittweise annähernde) Befragung der übergeordneten DNS-Server.

Damit also Ihr PC herausfinden kann, wie er den Web-Server der Berufsschule (www.bsinfo.eu.) erreicht, beauftragt er seinen lokalen DNS-Server und dieser in der Regel den DNS-Server des ISPs mit einer entsprechenden Recherche. Dieser fragt zunächst einen der Root-Server nach der IP-Adresse von 'www.bsinfo.eu.'. Der Root-Server kennt die IP nicht, weiß aber, welche DNS-Server für die TLD 'eu.' zuständig sind und teilt dem anfragenden DNS-Server diese mit, deligiert also die Anfrage im Namensraum eine Stufe nach unten! Der lokale DNS-Server fragt nun einen für die TLD zuständigen DNS-Server. Auch dieser kennt die IP von 'www.bsinfo.eu.' nicht, nennt aber die für die 2nd-Level-Domain 'bsinfo.eu.' zuständigen DNS-Server (erneute Deligierung) und so weiter, bis der lokale DNS-Server denjenigen DNS-Server findet, der tatsächlich die IP von 'www.bsinfo.eu.' in seiner Datenbank hat. Zuletzt gibt der lokale DNS-Server die IP dann zurück an den anfragenden Client.

Schematisches Prinzip iterativer DNS-Abragen



Erklären Sie was ein Cache ist und welchen Vorteil dieser im Zusammenhang mit DNS bietet!

Cache: _____

_____

Welche Nachrichtenart wird bei der Anfrage eines Root-Servers genutzt?

☐ Unicast ☐ Multicast ☐ Anycast

nslookup – Das Kommandozeilentool für DNS-Anfragen unter Windows

```
Syntax:
   nslookup [-opt ...]             # interaktiver Modus, Standardserver wird
                                     verwendet.
   nslookup [-opt ...] - server    # interaktiver Modus, der Server "server"
                                     wird verwendet.
   nslookup [-opt ...] host        # Der Host "host" wird gesucht,Standard-
                                     server wird verwendet
   nslookup [-opt ...] host server # Der Host "host" wird gesucht, der Server
                                     "server" verwendet.
```

Nennen Sie den korrekten nslookup Befehl für folgende Anfragen!

a) Root-Server kennen IPs der anderen Root-Server (s.o.) – Fragen Sie den 'f Root-Server' nach der IPv4-Adresse des 'a Root-Server'!

   Befehl: _____

Iterative Abfrage

b) Root-Server kennen die autoritativen (zuständigen) Server der TLDs (s.o.) – Fragen Sie einen der Root-Server nach den Nameservern, welche die TLD 'eu.' verwalten! Als Option (s.o. Syntax) benötigen sie zusätzlich '`-type=NS`'.
   Notieren Sie den Namen einer der Nameserver, die 'eu.' verwalten!

   Befehl: _____

   Nameserver 'eu.' und IP : _____

c) Fragen Sie einen der für 'eu' zuständigen Nameserver nach der 2nd-Level-Domain 'bsinfo.eu.'
   Notieren Sie den Namen einer der Nameserver, die 'bsinfo.eu' verwalten! Als Option benötigen sie zusätzlich '`-type=NS`'.

   Befehl: _____

   Nameserver 'bsinfo.eu.' und IP: _____

d) Fragen Sie einen der für 'bsinfo.eu.' zuständigen Nameserver nach der IP des Hosts 'www.bsinfo.eu'

   Befehl: _____

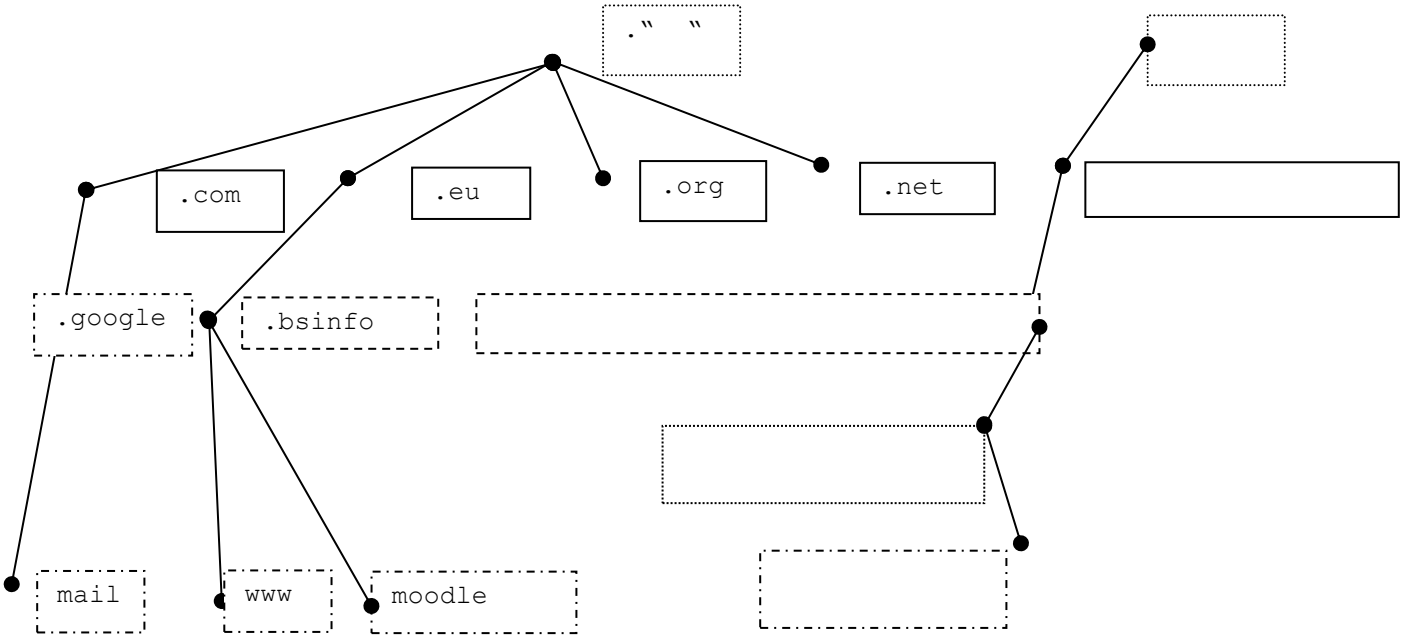
   IP von 'www.bsinfo.eu.' _____

e) Fragen Sie den Standardserver ihres Rechners (`'ipconfig /all' – 1.DNS-Server`) nach der IP des Hosts 'www.bsinfo.eu.'
   Worin unterscheiden sich die Antworten von d) und e) und warum?
   bei d): _____

   bei e): _____

Neben dem Mechanismus der iterativen Abfrage gibt es auch die Möglichkeit, dass DNS-Server an andere als die Root-Server weiterleiten, z.B. an den direkt übergeordneten DNS-Server (z.B. den des Providers). Wir erinnern uns: die dezentrale Auskunft ist ein Ziel (s.o). Dann spricht man von Weiterleitung, englisch Forwarding.

Der hierarchisch (von oben nach unten) aufgebaute DNS-Namensraum:



Was ist denn der FQDN?
Der FQDN (Fully Qualified Domain Name) setzt sich aus dem Hostname und dem Primären DNS-Suffix zusammen und identifiziert einen DNS-Client eindeutig im System.

Aufbau:
DNS-Hostname.[[Sub-Domain(s).]Sub-Domain.]Second-Level-Domain.Top-Level-Domain.root(" ")

kurz:

DNS-Hostname.Primäres_DNS_Suffix

Unterstreichen Sie für folgende Beispiele den DNS-Hostnamen in blau sowie die einzelnen Domain-Teile bis hin zu root!

`www.bsinfo.eu.`

`a.root-servers.net.`

`google.com.`

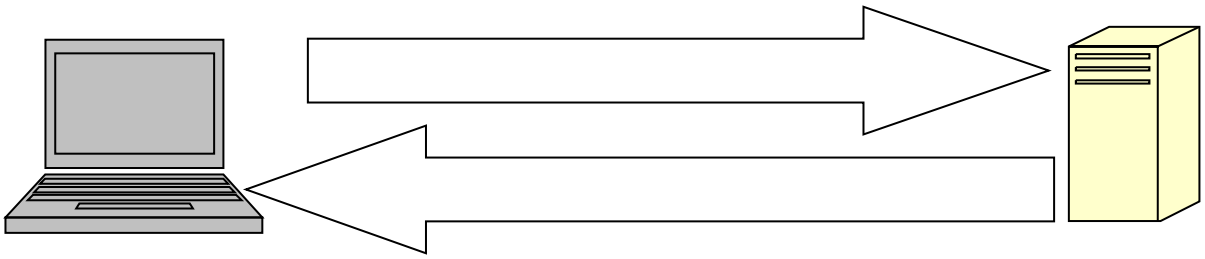
`http://ftp.heise.de.`

Merke: Das primäre DNS-Suffix gibt an,

DNS-Anfragearten

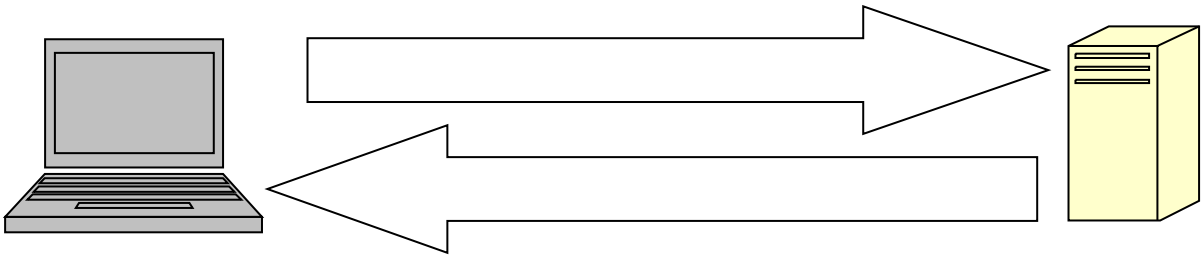
Ergänzen Sie die Pfeile um die zu übertragenen Frage- und Antwortsätze!

Die Forward-Lookup-Abfrage (A-Record):



Beispiel-Befehl in der CMD: _____

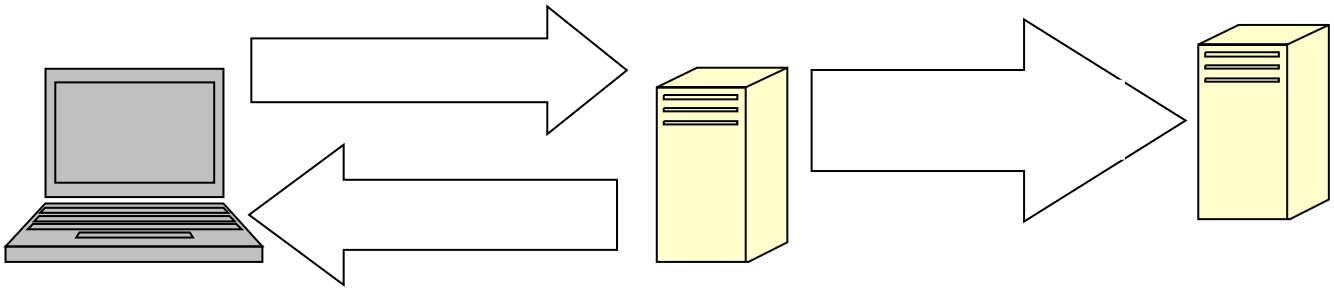
Reverse-Lookup-Abfrage (PTR-Record):



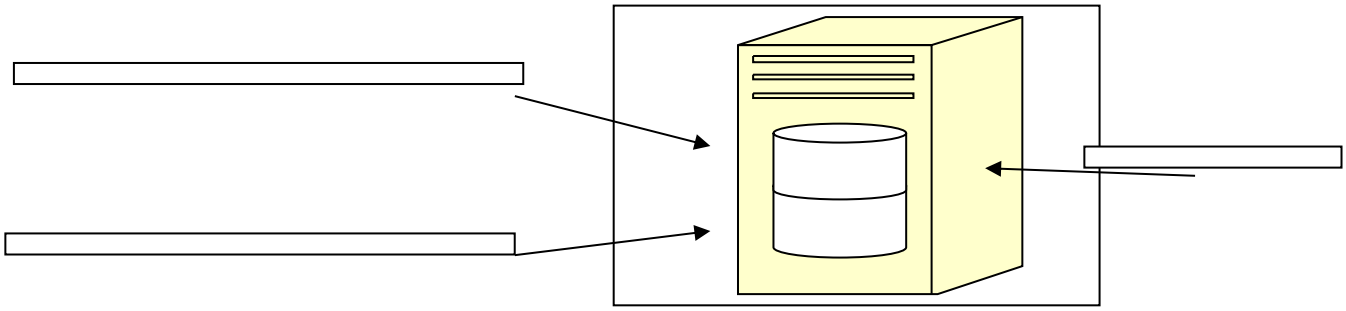
Beispiel-Befehl in der CMD: _____

Dynamisches DNS:

Dynamisches DNS bedeutet, dass ein DNS-Client Konfigurationsänderungen dem DNS-Server melden darf, der DNS-Server der Änderungsmeldung vertraut und diese umsetzt. Somit ist sichergestellt, dass die Namensauflösung immer korrekt funktioniert.
Ist der DNS-Client gleichtzeitig ein DHCP-Client, so erhält der DNS-Server auch vom DHCP-Server Änderungsmitteilungen!

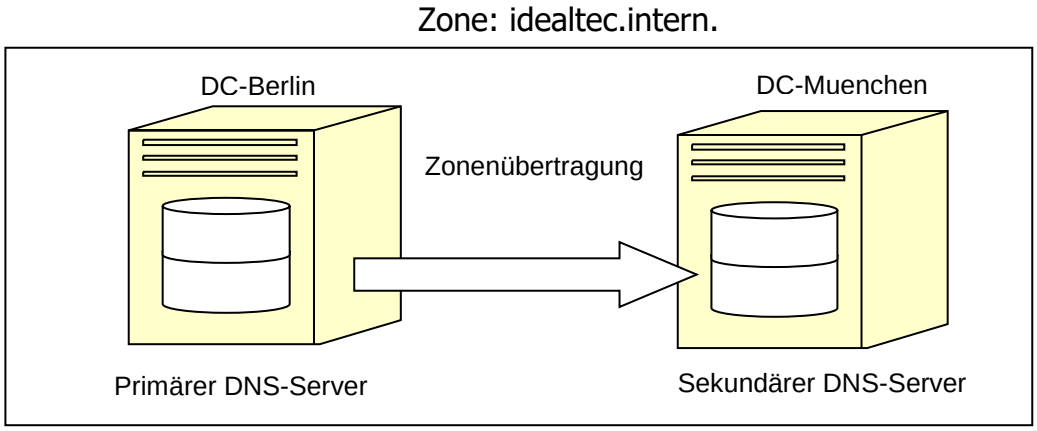


DNS-Zone – was ist das?



Informationen über die verwaltete(n) DNS-Zonen werden in einfachen Dateien gespeichert. Diese findet man auf Windows Systemen unter `c:\windows\system32\dns`.
Forward-Zonen-Dateien werden nach dem Muster `Domainname.dns` gebildet.
für z.B. die Domain `idealtec.intern` also: _____ ,
Reverse-Zonen-Dateien nach dem Muster `NetzadressanteilRrückwärts.in-addr.arpa.dns`
für z.B. das IP-Netz `192.168.0.0/24` also: _____

Zonenübertragung (Zone Transfer)



Bei der Zonenübertragung (-transfer) wird die DNS-Datenbank vom primären (primary) DNS-Server zum sekundären(secondary) 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.
WICHTIG: Der A-Rootserver ist KEIN primärer DNS-Server, der Prozess der Zonenübertragung findet auf Root-Ebene NICHT statt! Stattdessen, siehe S. 1 des Skripts sorgen auf Rootebene die *Root-Server Operatoren* in Zusammenarbeit mit Verisign für die Verteilung des *root zone files* !!!

Siehe Seite 3 kann man mit der `nslookup` Option `-type=NS` (NameServer) herausfinden, welche Nameserver für eine Domain zuständig sind, nicht jedoch, welcher Server der primäry DNS-Server der Domain ist. Hierfür benötigen Sie die Option `-type=SOA` (Start of Authority)!
Wie lautet der nslookup Befehl, um den primären DNS-Server von bsinfo.eu zu ermitteln?

.....

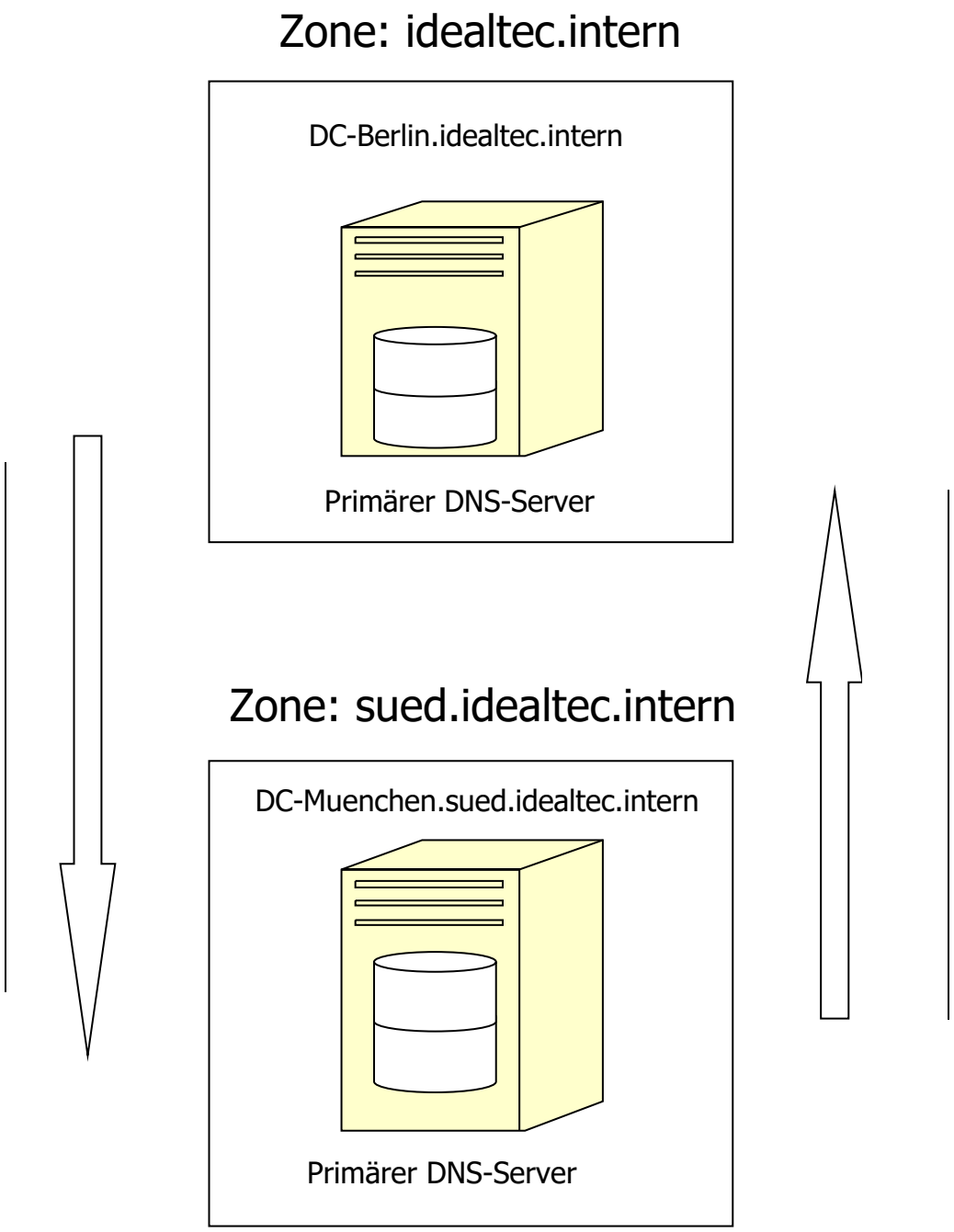
Vorteile der Zonenübertragung:

-
-
-

Begriff: *Zonendelegierung* und *Weiterleitung*

(Zone Delegation and Forwarding)

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 und Zonenweiterleitung:

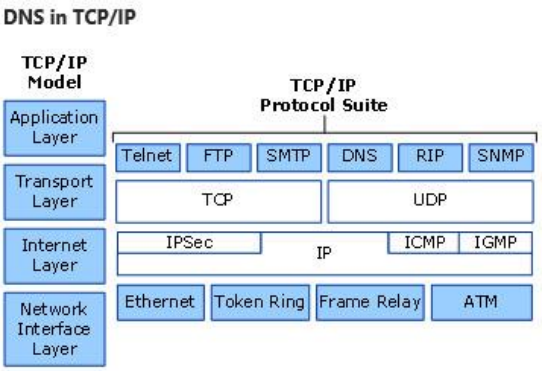
-
-

DNS Resource Records oder was steht in der Zonendatei drin?

Im Standardfall generiert ein **DNS-Server** seine interne Datenbank aus einer Textdatei, der sogenannten "**Zonen-Datei**". Damit er funktioniert, müssen bestimmte Einträge korrekt eingetragen worden sein. An dieser Stelle sollen nur ein paar grundlegende Eigenschaften der wichtigsten Typen von Resource Records betrachtet werden. Es gibt verschiedene Record-Typen:

- **SOA-Records** (Source of Authority) enthalten die technischen Angaben für die gesamte Zone, den Primären DNS-Server einer Zone sowie einige Steuerdaten für die Zusammenarbeit der Nameserver untereinander.
- **NS-Records** (Name Server) verweisen auf die Nameserver, die für eine Zone authoritativ sind. Auf den eigenen Namen zeigende NS-Records dienen der Plausibilitätsprüfung; NS-Records für eine Subdomain weisen darauf hin, dass die Informationen für die Subdomain auf einem anderen Nameserver zu finden sind (Delegation).
- **A-Records** (Address) verknüpfen einen Domainnamen mit einer IP-Adresse(Ipv4)
- ***AAAA-Records*** *(Address) für IPv6, verknüpfen einen Domainnamen mit einer IP-Adresse*
- **PTR-Records** (Pointer) verknüpfen eine IP-Adresse "rückwärts" mit einem Domainnamen.
- **CNAME**-Records Canonical Name) definieren einen Domainnamen als Alias für einen anderen. Es gibt also für jedes System einen A-Record und ggf. noch beliebig viele CNAME-Records.
- **MX-Records** (Mail Exchanger) definieren, bei welchen Rechnern Mail für eine Domain eingeliefert werden soll. Auf diese Weise sind generische Mailadressen wie z.B. "*mail@bsinfo.eu*" möglich.
- **TXT-Records** (Text) enthalten beliebige alphanumerische Informationen zu einem Domainnamen.

Quelle: https://www.cloudflare.com/de-de/learning/dns/dns-records/ abgerufen 25.07.2023 11:00Uhr



Die meisten Netzwerkdienste nutzen einen spezifischen Port auf OSI-Schicht 4. Die Zuordnung von Netzwerkdienst zu Port sind auf vielen Systemen hinterlegt in der Datei /etc/services (UX, Mac) bzw. in c:\windows\system32\drivers\etc\services (Windows).
Führen Sie folgenden Befehl in einer Shell aus und ermitteln Sie den /die Port(s), welche DNS nutzt!

DOS : `type c:\windows\System32\drivers\etc\services | findstr /i domain`

PS : `get-content c:\windows\System32\drivers\etc\services | Select-String -Pattern domain`

UX : `cat /etc/services | grep –i domain`

=> DNS Port: ___ Protokoll: _____

Sie haben vielleicht bemerkt, dass es für DNS sowohl einen Eintrag für UDP als auch TCP gibt.
Welches Protokoll wird also verwendet? – Beantworten Sie die Frage mit Hilfe des folgenden Textes: [1]

DNS is an application layer protocol. All application layer protocols use one of the two transport layer protocols, UDP and TCP. TCP is reliable and UDP is not reliable. DNS is supposed to be reliable, but it uses UDP, why?

1) UDP is much faster. TCP is slow as it requires a 3-way handshake.
2) DNS requests are generally very small (< 513 bytes) and fit well within UDP segments.
3) UDP is not reliable, but reliability can be added to the application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer.

Actually, DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server. When the length of the answer exceeds 512 bytes[2] and both client and server support EDNS (Extension Mechanism for DNS), larger UDP packets are used. Otherwise, the query is sent again using the Transmission Control Protocol (TCP). TCP is also used for tasks such as zone transfers. Some resolver implementations use TCP for all queries.

.....

.....

.....

.....

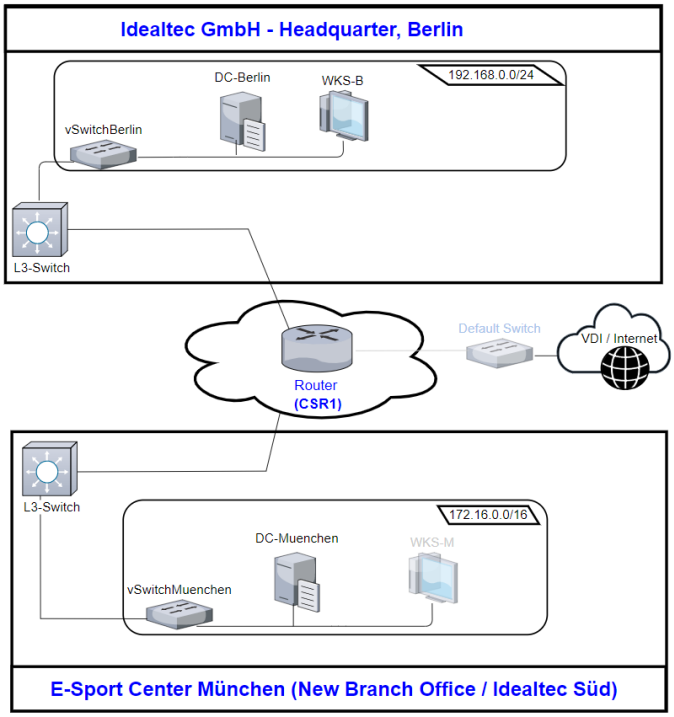
.....

.....

[1] entnommen von: https://www.geeksforgeeks.org/why-does-dns-use-udp-and-not-tcp/

[2] Beispiele von DNS Nachrichten > 512 bytes: https://www.infoblox.com/dns-security-resource-center/dns-security-faq/is-dns-tcp-or-udp-port-53/

1. Szenario der Fa. Idealtec GmbH: *Zonenübertragung*

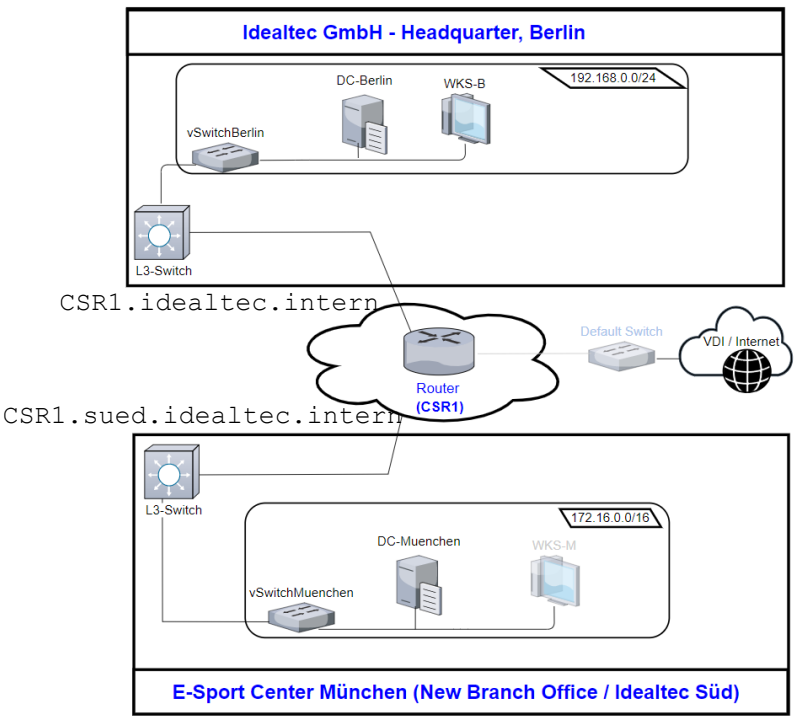


Was spricht aus technischer Sicht für dieses Szenario?

Was spricht für dieses Szenario?

Zeichnen Sie die Zone `idealtec.intern.` ein! Skizzieren Sie durch einen Pfeil, von wo nach wo die Zonenübertragung stattfindet!

2. Szenario: *Zonendelegierung* und *Weiterleitung*



Zeichnen Sie die Zonen `idealtec.intern` und `sued.idealtec.intern` ein!
Skizzieren Sie durch Pfeile von wo nach wo die *Delegierung* bzw. *Weiterleitung* erfolgt!
Wodurch unterscheiden sich Szenario 1 von Szenario 2?