# DNS Spick

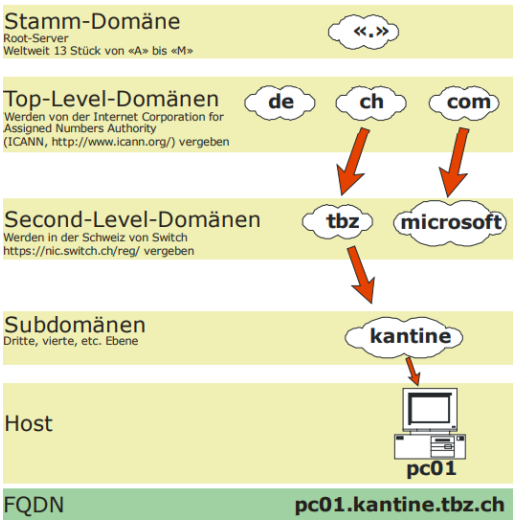
## Host Datei

Die Hosts-Datei ist dafür verantwortlich, dass jeder IP-Adresse ein Hostname zugeordnet wird. So ist auch jede Website bedingt mit einer IP-Adresse verbunden. Die IP-Adresse gehört dabei zum Server, über den die Website läuft.

Windows: C:\Windows\ System32\drivers\etc\hosts
Linux: [Ctrl] + [Alt] + [T] dann " sudo vi /etc/hosts "

## Namespace

Eine DNS-Domäne ist ein Namensraum der begrenzt wird durch den Inhalt der DNS-Datenbank, die als Zonendatei bezeichnet wird. Der DNS Name (FQDN) ist streng hierarchisch aufgebaut und wird von **hinten nach vorne** gelesen. **Die Stammdomäne (Root)** ist die oberste Domäne einer Hierarchie und verwendet eine Nullbezeichnung «.». Direkt unter der Stammdomäne befindet sich die erste Ebene **(Top-Level-Domains)**. Diese TLDs werden nach Organisationstyp oder nach Land eingeteilt. Auf der nächsten Ebene **(Second-Level-Domains)** können sowohl Hosts als auch Teildomänen (firma.ch) enthalten sein. Darunter liegen die Domänen der dritten, vierten, etc. Ebene.

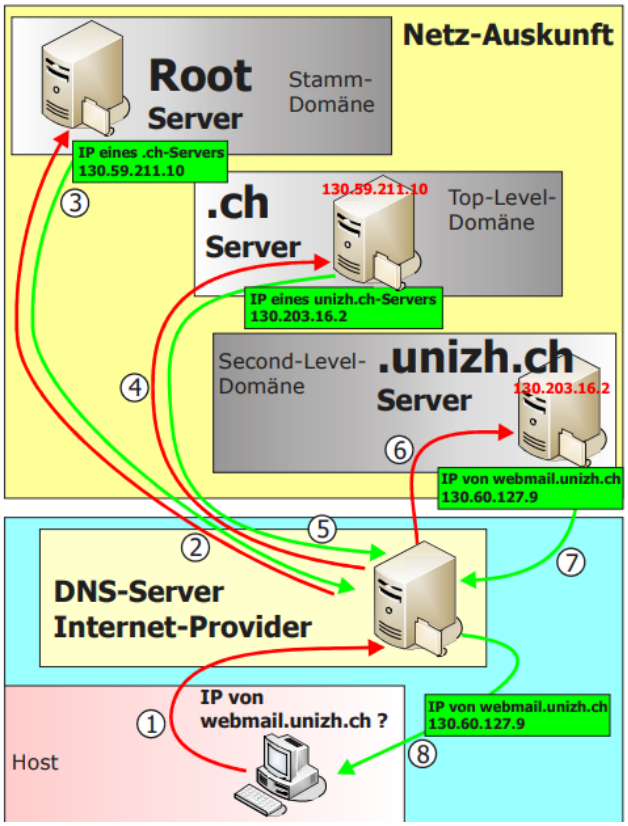



## FQDN

FQDN Der komplette DNS-Name («FQDN» = «Fully Qualified Domain Name») für einen Host besteht aus dem Hostnamen und dem DNS-Domänennamen. Der Computer «pc01» ist Host in der DNS-Domäne «kantine.tbz.ch».

## Name-Server

Name-Server Gibt man im eigenen Browser einen Domänennamen ein, stellt der Rechner eine Anfrage an den Namenserver. Im Internet ist dies in der Regel der Namenserver des Providers. Sind die angeforderten Namen dort nicht verfügbar, so wird die Anfrage zu einem anderen Namenserver weiter geleitet. Jeder Namenserver besitzt eine fest konfigurierte Liste der Root-Server. Dort beginnt jeweils die Suche nach einem Namen. Die Root-Server kennen alle Namenserver die Toplevel-Domänen verwalten. Ein DNS-Server tritt niemals alleine auf; es gibt immer einen Primary- und einen SecondaryNameserver. Sie sind voneinander unabhängig und redundant ausgelegt. Der Secondary gleicht in regelmässigen Abständen seine Daten mit dem Primary ab. Jeder DNS-Server hat einen Cache, in dem er erfolgreiche DNS-Anfragen abspeichert. Die gespeicherten Daten haben eine TTL von ca. 2 Tagen. **(Weltweit 13-Rootserver)**




## Richtlinien zum Erstellen des Domänennamespace

- Eine DNS-Struktur darf bis zu 5 Ebenen enthalten.
- Die Namen für Subdomänen einer Domäne müssen eindeutig sein.
- Die maximale Länge eines Domänennamens beträgt 63 Zeichen (inkl. Punkte).
- Die Gesamtlänge eines FQDN beträgt maximal 255 Zeichen.

## Ablauf

1. Der Nutzer gibt die URL einer Website (z. B. www.google.com) im Browser ein.
2. Der Resolver schickt eine Anfrage an einen DNS-Root-Server.
3. Der Root-Server gibt dem Resolver an, unter welcher Top-Level-Domain die Information für die Website zu finden ist. Im Fall von www.google.com handelt es sich um die Top Level Domain .com.
4. Der Resolver schickt eine Anfrage an die entsprechende Top Level Domain.
5. Der Server der Top Level Domain gibt die IP-Adresse des entsprechenden Nameservers an, woraufhin der Resolver eine Anfrage an den Nameserver schickt.
6. Der Nameserver sendet die IP-Adresse der entsprechenden Domain an den Resolver, welcher sie an den Browser weitergibt.
7. Der Browser ruft nun die Website auf, indem er eine HTTP-Anfrage an die IP-Adresse schickt. Der so angesprochene Server schickt die Dateien der Website an den Browser, sodass der Content angezeigt wird.

## Forward-Lookup / Reverse Lookup

Die Namensauflösung wird durch einen DNS Client (DNS resolver), der in die Applikation (z.B. Browser) eingebunden ist, initiiert. Ein Namenserver kann nur solche Namen auflösen, für die er autorisiert ist, d.h. für die er Einträge in seiner DNS-Datenbank besitzt. Erhält ein Namenserver eine Abfrage die er selbst nicht auflösen kann, übergibt er die Anfrage an einen übergeordneten (Root-)Namenserver.

Forward: Name zu IP-Adresse / Reverse: IP-Adresse zu Name

## rekursiv

wenn der client eine abfrage an seinen dns server stellt, dieser den namen nicht lokal auflösen kann, so stellt er eine abfrage an einem ihn bekannten dns server, der antwortet dann eventuell mit einer namensauflösung oder auch mit einem verweis auf einen dns server, den dein dns server dann befragen würde usw. bis er den namen hat und dann an den client weitergibt.

## iterativ

du stellst ne anfrage an dein dns server, der kann ihn nicht lokal auflösen, fragt aber keine weitere dns server ab, sondern schickt den client einen verweis auf einen anderen dns server den er fragen soll.

## Protokoll

DNS ist auf der Anwendungsschicht des OSI-Modells angeordnet. Es nutzt zur Übertragung TCP und UDP auf dem Port 53**. In der Regel verwendet der Resolver das UDP-Protokoll. Wenn die Antwort grösser als 512 Byte gross ist, werden nur 512 Byte übertragen. Anschliessend muss der Resolver seine Anfrage noch einmal über TCP wiederholen, damit die Antwort in mehrere Segmente aufgeteilt werden kann.** Der Datenaustausch zwischen Primary- und Secondary-DNS-Server wird nur mit TCP geregelt.

## Zonen

**Zonenname**: Üblicherweise wird eine Zone nach der höchsten Domäne in der Hierarchie benannt, der die Zone angehört (z.B. ch-Zone).

**Zonendatei**: Die Zonendatei beinhaltet alle Daten für die Namensauflösung. Standardmässig wird der Zonenname mit der Erweiterung .dns versehen. Wenn der Zonenname beispielsweise firma.ch lautet, wird als Standardname für die Zonendatenbankdatei der Name firma.ch.dns verwendet. Die Datei wird im Verzeichnis «C:\WINDOWS\System32\DNS» gespeichert.

**Zonentyp**:

Primär: In einer primären Zone wird die Original-Zonendatei von einem primären DNS Server verwaltet.

Sekundär: In einer sekundären Zone kopiert ein sekundärer DNS-Server die Zonendatei eines anderen Servers, der wiederum primär oder sekundär sein kann. Das gewährleistet eine Redundanz und verteilt die Last der Namensauflösung.

Active Directory-integriert: Die Zonendatei wird im Active Directory gespeichert. Bei der Active Directory-Verzeichnisreplikation werden nur die relevanten Änderungen übermittelt. Daher ist sie schneller und effizienter als die Standard-DNS-Replikation.

| | | |
|---|---|---|
| Root | Root-Server | DNS-Server der obersten Hierarchie-Ebene. Zuständig für die Root-Domäne. Jeder DNS-Server muss die Root-Server kennen. |
| Zone | Primärer DNS-Server | Übernimmt die Zuständigkeit für eine (oder mehrere) Zonen. Er ist für die betreffenden Zonen autorisierend. |
| Zone | Sekundärer DNS-Server | Ist abhängig vom primären DNS-Server. Er holt sich regelmässig Kopien der DNS-Datenbank vom primären DNS-Server. Er hat zwei Möglichkeiten um das zu machen:<br>Er lädt die komplette Zonendatenbank herunter (AXFR).<br>er lädt nur Änderungen innerhalb eines bestimmten Zeitintervalls herunter (IXFR).<br>Der sekundäre DNS-Server ist nicht autorisierend. Er kann keine Änderungen an der Zonen-Datenbank vornehmen. Er dient nur der besseren Verfügbarkeit des Dienstes und dem Lastausgleich. |
| Zone | Active Directory DNS-Server | Existiert nur auf Windows-Domänencontrollern. |
| | Caching-Only-DNS-Server | Speichert keine Zonendatenbank. Erhält keine Aktualisierung von einem primären DNS-Server. Dient nur dem Zwischenspeichern der Abfragen um den Netzwerkverkehr zu entlasten. |
| | Weiterleitende DNS-Server (Forwarder) | Leiten Anfragen weiter, die sie selbst nicht beantworten können. |

**CMD Befehle**

ipconfig/ flushdns = DNS Cache leeren

ipconfig/ displaydns = DNS Verlauf anzeigen

nslookup= Um IP-Adressen oder Domains eines bestimmten Computers mittels DNS herauszufinden.

dnslookup: Name DNS Server.

| C:\WINOWS\system32\dns\ | |
|---|---|
| soltec.intern.dns | Zonendatenbankdatei für Forward-Lookup-Abfragen in der Zone soltec.<br>Die Datenbank ist nach Hostnamen indiziert. |
| 100.168.192.in-addr.arpa.dns | Zonendatenbankdatei für Reverse-Lookup-Abfragen in der Zone *soltec*.<br>Die Datenbankdatei ist nach IP-Adressen indiziert. |
| cache.dns | In dieser Datei werden Ergebnisse von Namensauflösungen gespeichert, die für eine begrenzte Zeit zur Namensauflösung herangezogen werden. |
| root.dns | Diese Datei ist optional und wird vom Stammnamensserver gepflegt. Sie steuert das Starten des DNS-Dienstes. |