



## Reverse Lookup

Hier wird eine IP-Adresse wieder einem Hostnamen zugeordnet.

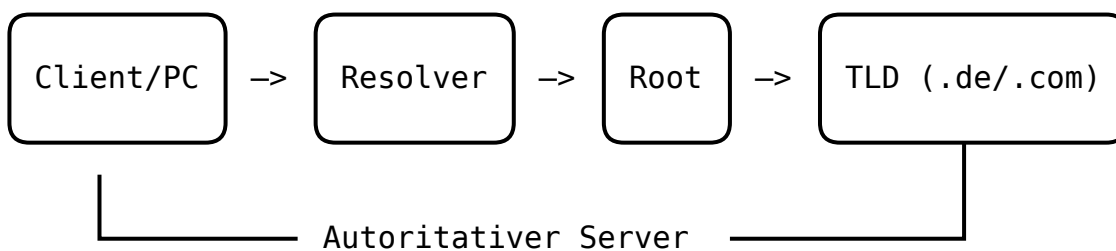
Beispiel:

- Anfrage: 34.216.184.93.in-addr.arpa
- Antwort: [www.example.com](http://www.example.com)

## DNS-Record-Typen

Typ	Bedeutung	Beispiel
<b>A</b>	IPv4-Adresse	www → 93.184.216.34
<b>AAAA</b>	IPv6-Adresse	www → 2606:2800:220:1:248:1893:25c8:1946
<b>CNAME</b>	Alias auf anderen Namen	www → server01.example.com
<b>MX</b>	Mailserver	example.com → mail.example.com
<b>TXT</b>	Frei definierbare Texte	SPF, DKIM, Verifizierungen
<b>NS</b>	autoritative Nameserver	example.com → ns1.example.com
<b>PTR</b>	Reverse Lookup	34.216.184.93 → <a href="http://www.example.com">www.example.com</a>
<b>SRV</b>	Dienste (SIP, Kerberos, AD)	kerberos.tcp.example.com
<b>SOA</b>	Verwaltungsdaten der Zone	Serial, Refresh usw.

## Ablauf einer DNS-Auflösung (Query Flow)



Der Resolver (meist der Router oder ein DNS-Server im LAN) kümmert sich um Caching, Wiederholungen und Validierung.

## DNS-Caching

DNS speichert Antworten für eine bestimmte Zeit (TTL). Dadurch werden:

- Netzwerke entlastet
- Ladezeiten verkürzt

- Autoritative Server geschont

Beispiel TTL:

- 3600 Sekunden = 1 Stunde

---

## Zonen & Zonen-Dateien

Eine **DNS-Zone** ist ein Teilbaum des Namensraums, verwaltet von einem autoritativen Server.

Typische Zonendatei (BIND-Stil):

```
$TTL 3600
@ IN SOA ns1.example.com. admin.example.com. (
2024112701 ; Serial
3600      ; Refresh
600      ; Retry
604800   ; Expire
86400 )   ; Minimum
IN NS ns1.example.com.
www IN A  93.184.216.34
mail IN MX 10 mail.example.com.
```

---

## Sicherheit: DNSSEC

DNSSEC schützt vor Spoofing und Man-in-the-Middle-Angriffen.

DNSSEC bietet:

- **Authentizität der Daten**
- **Integrität**
- **Chain of Trust** → Root → TLD → Domain

Keine Verschlüsselung – nur Signaturen!

---

## DNS Spoofing & Angriffe

Typische Angriffe:

- Cache Poisoning
- DNS-Spoofing
- DDoS via offene Resolver
- Subdomain Takeover
- Gefälschte Zonen (z. B. durch offenen AXFR)

Basic-Härtung:

- AXFR nur für autorisierte IPs
  - DNSSEC aktivieren
  - Rekursion LAN-only
  - Rate Limiting
  - Keine offenen Resolver
- 

## Tools für DNS-Analyse

- dig - der Klassiker
- nslookup - legacy, aber noch gebräuchlich
- host - einfaches Lookup
- drill - modern, DNSSEC-tauglich
- tcpdump - Paketmitschnitt

Beispiele:

```
dig A example.com
dig +trace www.example.com
dig -x 93.184.216.34
```

---

## Beispiel: DNS + DHCP im Zusammenspiel

DHCP kann DNS-Einträge automatisch erzeugen (DDNS):

- Client bekommt IP → DHCP-Server aktualisiert DNS
- Gängig in Active-Directory-Umgebungen
- Erhöht Übersicht & Automatisierung

## Zusammenfassung

DNS ist die zentrale Komponente der Namensauflösung. Es ist global verteilt, hochverfügbar,

leistungsfähig und unverzichtbar. Eine saubere DNS-Konfiguration entscheidet oft über Erreichbarkeit, Sicherheit und Performance.



**Ein Admin, der DNS beherrscht, hat die halbe  
Netzwerkwelt verstanden - der Rest ist nur Routing ...  
und Kaffee.**

From:

<http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:

<http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:dns&rev=1764322132>

Last update: **28.11.2025 10:28**

