DNS (Domain Name System)

Domain Name System (DNS) je hierarchický, distribuovaný systém pro správu názvů domén a jejich překlad na IP adresy. V počítačových sítích plní roli „adresáře“, který umožňuje lidem používat čitelné názvy (např. `www.google.com`) namísto numerických IP adres (např. `172.217.16.196`).

DNS běží primárně na portu **53** a využívá protokoly **UDP** (pro běžné dotazy) a **TCP** (pro přenosy zón a velké odpovědi).

1. Hierarchická struktura Systém je organizován jako obrácený strom:

- **Root zone (Kořenová zóna):** Označuje se tečkou `.`. Spravuje ji organizace ICANN.
- **TLD (Top-Level Domain):** Horní úrovně domén, např. `.cz`, `.com`, `.org`.
- **Second-Level Domain:** Samotný název registrovaný subjektem (např. `seznam` v `seznam.cz`).
- **Subdomény:** Další úrovně definované vlastníkem (např. `blog.firma.cz`).

2. Proces rozlišení (DNS Resolution) Když klient (tzv. **Stub Resolver**) odešle dotaz, proběhne následující cyklus:

```
1. **Recursive Resolver:** Server vašeho ISP nebo veřejný (8.8.8.8) přijme
dotaz.
2. **Root Nameservers:** Resolver se zeptá kořene, kde najde TLD (např.
''.cz'').
3. **TLD Nameservers:** Resolver se zeptá serverů ''.cz'', kde najde
autoritativní server pro danou doménu.
4. **Authoritative Nameservers:** Poslední článek, který vrací finální IP
adresu.
```

3. Typy DNS záznamů (Resource Records) V zónových souborech se setkáváme s těmito klíčovými typy:

Typ	Název	Význam
A	Address	Mapuje doménu na IPv4 adresu.
AAAA	IPv6 Address	Mapuje doménu na IPv6 adresu.
CNAME	Canonical Name	Alias pro jinou doménu (nasměruje jeden název na druhý).
MX	Mail Exchange	Určuje poštovní servery pro doménu.
TXT	Text Record	Libovolný text (využití pro SPF, DKIM, ověření domény).
NS	Name Server	Určuje, které servery jsou pro zónu autoritativní.
SOA	Start of Authority	Obsahuje klíčové info o zóně (e-mail správce, sériové číslo).
PTR	Pointer	Reverzní záznam (převod IP na název).

4. TTL a Caching **TTL (Time to Live)** určuje v sekundách, jak dlouho má být záznam uložen v mezipaměti (cache) resolverů.

- **Nízké TTL:** Umožňuje rychlé změny, ale zvyšuje zátěž serverů.
- **Vysoké TTL:** Zvyšuje rychlost (odpověď z cache), ale prodlužuje propagaci změn.

5. Technická diagnostika Pro testování DNS se v CLI používají nástroje jako `dig` nebo `nslookup`.

Příklad dotazu na MX záznamy:

```
dig seznam.cz MX +short
```

Příklad sledování cesty dotazu (iterativní dotazování):

```
dig +trace www.google.com
```

6. Bezpečnost: DNSSEC Standardní DNS není šifrované ani autentizované, což umožňuje útoky typu **DNS Spoofing** (podvržení adresy). **DNSSEC** (DNS Security Extensions) přidává k záznamům digitální podpisy. Tím zajišťuje, že data nebyla cestou změněna a pocházejí ze správného zdroje.

> **Varování:** DNSSEC neřeší soukromí (data jsou stále čitelná), řeší pouze integritu a autenticitu dat. Pro soukromí se používá **DoH** (DNS over HTTPS) nebo **DoT** (DNS over TLS).

Zpět na Sítě