# DNS, funkce, hierarchie DNS (od souboru po globální DNS servery), konfigurace

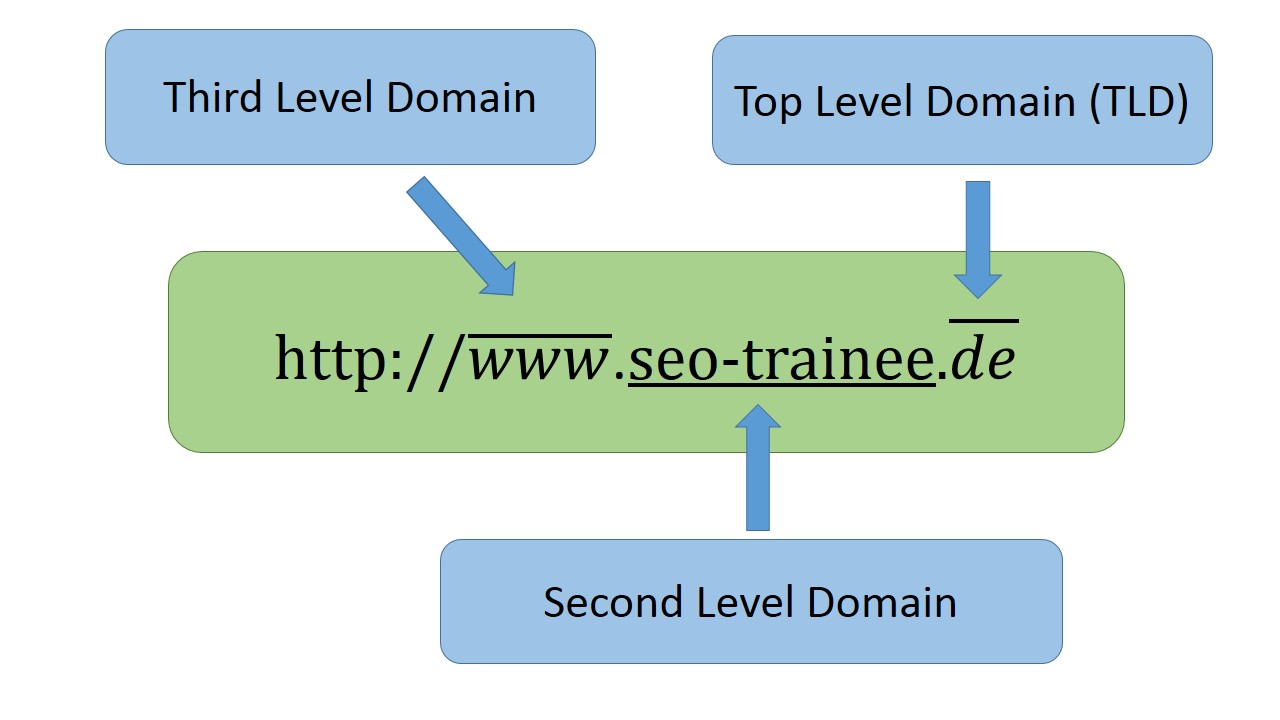
## DNS (TCP/53, UDP/53) RFC1035

Domain Name System je hierarchycký, decentralizovaný systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de facto jako distribuovaná databáze síťových informací.

Jména domén umožňují lepší orientaci lidem, adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (IPv4) – **A záznam** – nebo 128bitových (IPv6) – **AAAA záznam**. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno – **PTR záznam**.

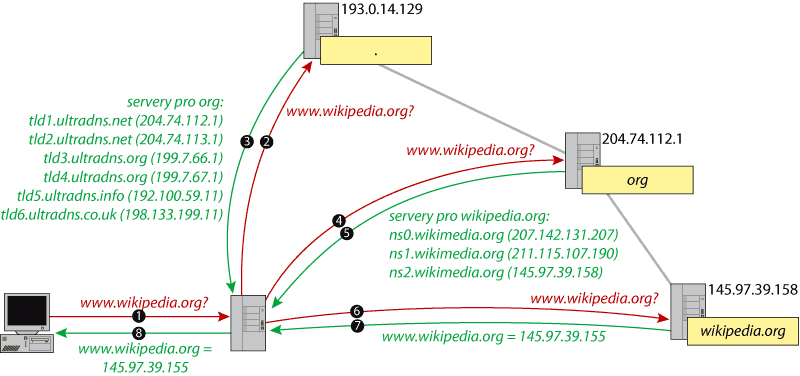
### DNS server

* **Autoritativní server** je ten, na němž jsou trvale uloženy záznamy k dané doméně/zóně. Autoritativních serverů je obvykle více (minimálně dva – primární a sekundární, ale běžně i více) a až na velmi speciální případy se na všech udržují totožné záznamy, tzn. každou změnu v záznamech je potřeba propagovat na všechny autoritativní servery. Autoritativní DNS servery jsou obvykle provozovány registrátorem domény nebo poskytovatelem webhostingu.
* **Rekurzivní (caching only)** server je server, na který se se svými dotazy obracejí klientská zařízení (počítač, mobil aj.). Server pro ně příslušný záznam získá rekurzivními dotazy u autoritativních DNS serverů a po stanovenou dobu (definovanou pomocí parametru TTL Time to live) je má uloženy v cache, aby mohl odpovídat klientům rychleji a šetřil zatížení serverů autoritativních. Na tomto serveru nejsou žádné zóny uloženy trvale. Rekurzivní DNS server se také stará o validaci DNSSEC, pokud tuto technologii podporuje. Rekurzivní DNS server obvykle provozuje ISP (poskytovatel připojení k internetu). Rekurzivních serverů může být na klientu definováno více na různých IP adresách, ale v praxi se spíše zajišťuje vysoká dostupnost serveru na první definované IP adrese. Informaci o DNS serverech na dané síti klient zjišťuje nejčastěji přes protokol DHCP, na IPv6 přes NDP
* **Root server** kořenové servery představují zásadní část technické infrastruktury interneu, na které závisí spolehlivost, správnost a bezpečnost operací na internetu. Tyto servery poskytují kořenový zónový soubor (root zone file) ostatním DNS serverům. Jsou součástí DNS, celosvětově distribuované databáze, která slouží k překladu unikátních doménových jmen na ostatní identifikátory.
  + Kořenový zónový soubor popisuje, kde se nacházejí autoritativní servery pro domény nejvyšší úrovně. Tento kořenový zónový soubor je relativně velmi malý a často se nemění – operátoři root serverů ho pouze zpřístupňují, samotný soubor je vytvářen a měněn organizací IANA.



### Zpsob získávání ipadresy

1. Uživatel zadal do svého [WWW klienta](https://cs.wikipedia.org/wiki/Webov%C3%BD_prohl%C3%AD%C5%BEe%C4%8D) doménové jméno *www.wikipedia.org*. Resolver v počítači se obrátil na lokální DNS server s dotazem na IP adresu pro *www.wikipedia.org*.
2. Lokální DNS server tuto informaci nezná. Má však k dispozici adresy kořenových serverů. Na jeden z nich se obrátí (řekněme na 193.0.14.129) a dotaz mu přepošle.
3. Kořenový server také nezná odpověď. Ví však, že existuje doména nejvyšší úrovně *org* a jaké jsou její autoritativní servery, jejichž adresy tazateli poskytne.
4. Lokální server jeden z nich vybere (řekněme, že zvolí *tld1.ultradns.net* s IP adresou 204.74.112.1) a pošle mu dotaz na IP adresu ke jménu *www.wikipedia.org*.
5. Oslovený server informaci opět nezná, ale poskytne IP adresy autoritativních serverů pro doménu *wikipedia.org*. Jsou to *ns0.wikimedia.org* (207.142.131.207), *ns1.wikimedia.org* (211.115.107.190) a *ns2.wikimedia.org* (145.97.39.158).
6. Lokální server opět jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu *www.wikipedia.org*.
7. Jelikož toto jméno se již nachází v doméně *wikipedia.org*, dostane od jejího serveru nepochybně autoritativní odpověď, že hledaná IP adresa zní 145.97.39.155.
8. Lokální DNS server tuto odpověď předá uživatelskému počítači, který se na ni ptal.



### Reverzní dotaz

Tento nesoulad řeší DNS tak, že při reverzních dotazech obrací pořadí bajtů v adrese. K obrácené adrese pak připojí doménu in-addr.arpa a výsledné „jméno“ pak vyhledává standardním postupem. Hledá-li například jméno k IP adrese 145.97.39.155, vytvoří dotaz na 155.39.97.145.in-addr.arpa. Obrácení IP adresy umožňuje delegovat správu reverzních domén odpovídajících sítím a podsítím správcům dotyčných sítí a podsítí. V příkladu použitou síť 145.97.0.0/16 spravuje nizozemský SURFnet a ten má také ve správě jí odpovídající doménu 97.145.in-addr.arpa. Kdykoli zavede do sítě nový počítač, může zároveň upravit data v reverzní doméně, aby odpovídala skutečné situaci.

### Záznamy

* **A** (**a**ddress record) obsahuje IPv4 adresu přiřazenou danému jménu, například když jménu *cosi.kdesi.cz* náleží IP adresa 1.2.3.4, bude zónový soubor pro doménu *kdesi.cz* obsahovat záznam

cosi IN A 1.2.3.4

* **AAAA** (IPv6 address record) obsahuje IPv6 adresu. Zmíněnému stroji bychom IPv6 adresu 2001:718:1c01:1:02e0:7dff:fe96:daa8 přiřadili záznamem

cosi IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8

* **CNAME** (**c**anonical **name** record) je alias - jiné jméno pro jméno již zavedené. Typicky se používá pro servery známých služeb, jako je například WWW. Jeho definice pomocí přezdívky umožňuje jej později snadno přestěhovat na jiný počítač. Pokud náš *cosi.kdesi.cz* má sloužit zároveň jako *www.kdesi.cz*, vložíme do zónového souboru

www IN CNAME cosi

* [**MX**](https://cs.wikipedia.org/wiki/MX_z%C3%A1znam) (**m**ail e**x**change record) oznamuje adresu a prioritu serveru pro příjem elektronické pošty pro danou doménu. Tentokrát jsou parametry dva – priorita (přirozené číslo, menší znamená vyšší prioritu) a doménové jméno serveru. Pokud poštu pro počítač *cosi.kdesi.cz* přijímá nejlépe počítač *mail.kdesi.cz* a případně jako záložní i *mail.jinde.cz*, bude zónový soubor obsahovat záznamy (všimněte si použití jmen s tečkou a bez tečky)

cosi IN MX 10 mail

IN MX 20 mail.jinde.cz.

* **NS** (**n**ame **s**erver record) ohlašuje jméno autoritativního DNS serveru pro danou doménu. Bude-li mít doména *kdesi.cz* poddoménu *obchod.kdesi.cz*, jejímiž servery budou *ns.kdesi.cz* (primární) a *ns.jinde.cz* (sekundární), bude zónový soubor pro *kdesi.cz* obsahovat

obchod IN NS ns

IN NS ns.jinde.cz.

* **PTR** (**p**oin**t**e**r** record) je speciální typ záznamu pro reverzní zóny. Obsahuje na pravé straně jméno počítače přidělené adrese na straně levé (adresa je transformována na doménu výše popsaným postupem). Držme se našeho příkladu pro záznam typu A – v souladu s ním by zónový soubor pro doménu *3.2.1.in-addr.arpa* měl obsahovat (zónový soubor definuje reverzní doménu, proto je třeba psát na pravé straně kompletní jméno s tečkou, jinak by za ně připojil reverzní doménu)

4 IN PTR cosi.kdesi.cz.

* **SOA record:** SOA stands for "start of authority." It's an important DNS record type that stores admin information about a domain. This information includes the email address of the admin and when the domain was last updated.
* **TXT record:** TXT stands for "text," and this record type lets the owner of a domain store text values in the DNS. Several services use this record to verify ownership of a domain.
* **PTR record:** A pointer (PTR) record provides a domain name for reverse lookup. It's the opposite of an A record as it provides the domain name linked to an IP address instead of the IP address for a domain.
* **SRV record:** Using this DNS record type, it's possible to store the IP address and port for specific services.
* **CERT record:** This record type stores public keys certificates.
* **DCHID:** This DNS record type stores information related to dynamic host configuration protocol (DHCP).
* **DNAME:** The full meaning of DNAME is "delegation name." This record type works very similarly to CNAME; however, it points all the subdomains for the alias to the canonical domain name. That is, pointing the DNAME for secondsite.com to example.com will also apply to staff.secondsite.com and any other subdomain.

Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén.

## DNS on computer file

* /etc/hosts … on linux dns local file (ip domain)
* /etc/resolve/conf … definuje se adresa dns a domena
* Hosts windows on dns local file

Nejdříve žádný DNS neexistoval jen se udržoval centrálně jeden soubor který si uživatelé dávali do /etc/hosts ale to se v jednu chvíli stalo neudržitlné a proto bylo potřeba vymyslet nějakou alternativu. Tedy DNS decentralizovaný sistém vznikl.

## DNS server konfigurace

1. sudo apt install dnsmasq
2. sudo nano /etc/dnsmasq.conf

# Never forward plain names (without a domain)

domain-needed

# Turn off DHCP on eth0

no-dhcp-interface=eth0

# Never forward addresses in the non-routable address space (RFC1918)

bogus-priv

# Add domain to host names

expand-hosts

# Domain to be added if expand-hosts is set

domain=zola.home

# Local domain to be served from /etc/hosts file

local=/zola.home/

# Don't read /etc/resolv.conf (I deleted it). Get the external name server from this file, see 'server' below

no-resolv

# External server, works with no-resolv

server=8.8.8.8