

Domain Name Service



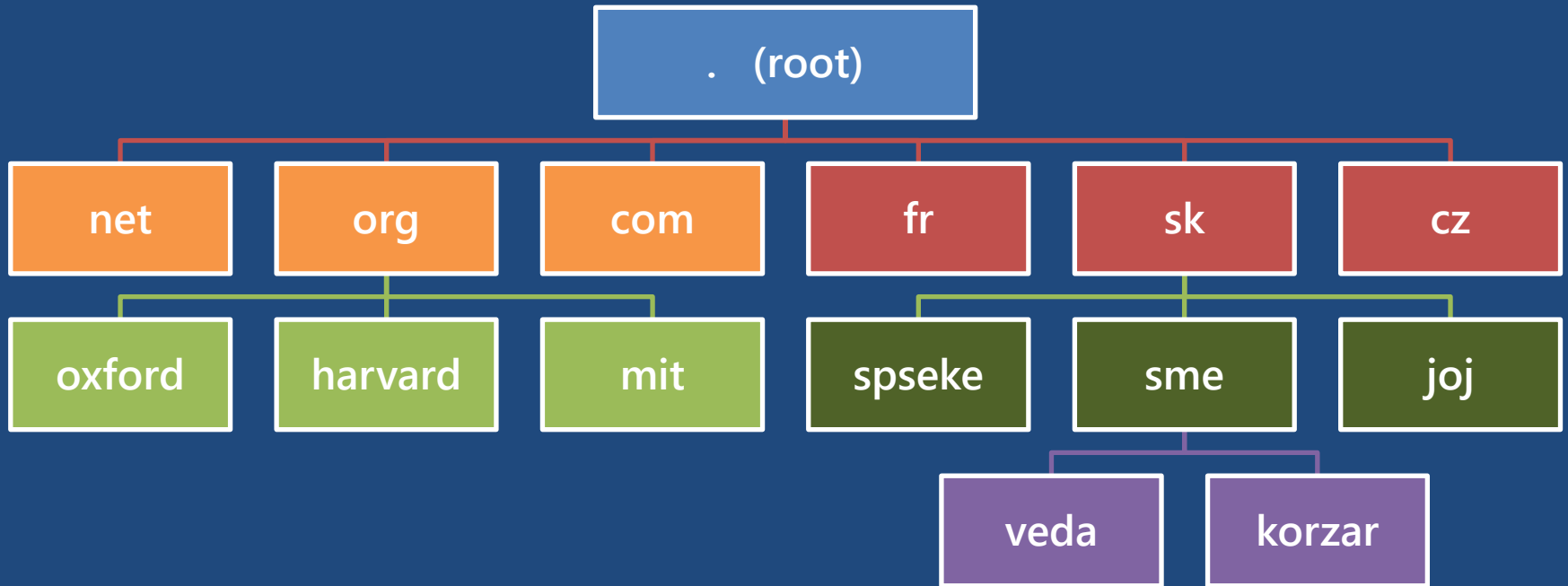
DNS

- Je to protokol s hierarchiou klient-server
- Počítače sa medzi sebou poznajú (komunikujú) na základe IP adries, ľudia si však lepšie pamätajú slovné názvy
- Ponúka zariadeniam využívajúcim IP protokol preklad doménových mien na IP adresy a naopak
- Nahrádza pôvodné HOSTS súbory

DNS

- Má distribuovanú databázu (tj. celý menný priestor sa nenachádza na 1 počítači ale je rozložený na viacerých serveroch)
- Databáza je hierarchická
- Mapovanie IP na mená môže byť statické alebo dynamické

Menný priestor



1. úroveň (TLD) - .sk

2. úroveň – sme.sk

3. úroveň – veda.sme.sk

národné - .sk, .cz

generické - .com, .net

Root DNS servery



Ako to funguje?

- DNS klient, nazývaný resolver sa pýta (posiela query) serveru a ten odpovedá (posiela response)
- Odpovedá buď autoritatívnym záznamom (t.j. ak má priamo vo svojej konfigurácii uvedené príslušné záznamy) alebo neautoritatívnym záznamom (ak ťahá údaje z cache, alebo z cudzieho DNS servera, ktorý sám doménu nespravuje)

Ako to funguje?

- V počítači máte v konfigurácii TCP/IP nastavenú IP adresu DNS servera
- Ak zadáte do prehliadača adresu stránky (napr. www.t-systems.sk), prehliadač odošle požiadavku operačnému systému
- Operačný systém sa pozrie do svojej lokálnej DNS cache (`ipconfig /displaydns`), či nemá záznam
- Ak taký záznam nemá, vytvorí požiadavku (a pridá na koniec adresy bodku) a odošle ju cez počítač (resolver) na zadanú IP DNS servra

Ako to funguje?

- Lokálny DNS (LDNS) server zistí, či je pre danú doménu autoritatívny, teda či má záznam o takomto preklade (resp. či ho môže poskytnúť)
- Ak nie, pošle ho na root (to je tá posledná bodka, ktorú pridal OS) a ten mu (LDNS) odpovie, kto je autoritatívny server pre doménu prvej úrovne (.sk)

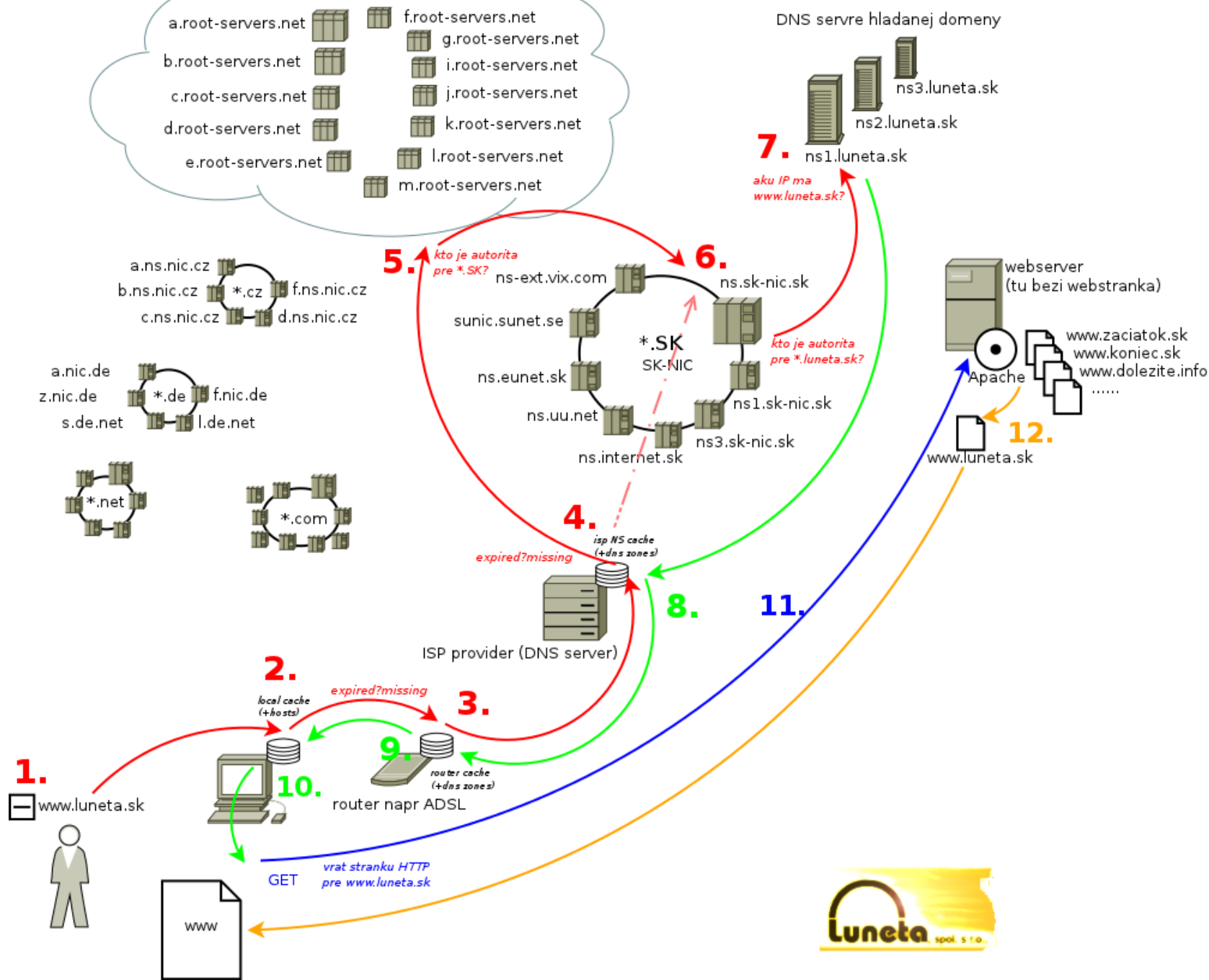
Ako to funguje?

- LDNS sa opýta autoritatívneho DNS servera pre doménu .sk (spravuje spoločnosť SK-NIC), kto je autoritatívny server pre doménu t-systems.sk
- Následne sa LDNS spojí s autoritatívnym serverom pre doménu t-systems.sk a ten mu pošle IP adresu servera, s názvom www.t-systems.sk

Ako to funguje?

- LDNS následne odpovie na žiadosť resolvera (nášho počítača) a odošle mu preklad doménového mena na IP adresu
- Operačný systém resolvera odošle odpoveď prehliadaču a ten už následne pošle HTTP GET požiadavku na IP adresu WEB servera (s adresou www.t-systems.sk), čím sa celý DNS proces ukončí

Ako funguje DNS ?



Domény a zóny

- Doména je tvorená skupinou počítačov (resp. ich mien), ktoré majú spoločnú pravú časť svojho doménového mena (napríklad spseke.sk).
- Dáta o doméne uložené na name serveri sú nazývané zóna. Zóna teda predstavuje len časť domény, je to teda časť priestoru mien, ktorú obhospodaruje jeden name server.
- Ak celá doména sídli na jednom serveri, doména a zóna sú synonymá

Domény a zóny

- Dotazovanie na server je vlastne dotazovanie na zónové záznamy
- Zónové záznamy sú plaintextové ASCII súbory, ktoré obsahujú údaje o name serveroch, údaje o mail serveroch, názvy (PQDN) hostov a iné údaje
- Každý záznam je tvorený názvom, typom a hodnotou

Najčastejšie typy záznamov

- SOA – start of authority – určuje základné údaje o doméne

```
@ IN SOA skola.internal.  admin.skola.internal. {  
    64          ; poradové číslo záznamu  
    3600        ; refresh záznamov na ostatných serveroch  
                  za hodinu (3600 sekúnd)  
    300         ; pri neúspešnom refreshi opakovaný  
                  pokus o 5 minút  
    172800      ; exspirácia záznamu na ostatných  
                  serveroch o 2 dni pri neúspešnom refreshi  
    43200       ; 12 hodín TTL záznamu v cache  
}
```

Najčastejšie typy záznamov

- NS – name server – určuje DNS servery, ktoré obsahujú údaje o doméne (zóne)

@ IN	NS	ns.skola.internal
@ IN	NS	ns.sanet.sk

- Záznamy sa najprv vyhľadávajú na DNS serveri ns.skola.internal a ak sa nenájdu (neexistujú alebo server nie je dostupný), hľadajú sa na DNS serveri ns.sanet.sk

Najčastejšie typy záznamov

- MX – slúži na definíciu servera prijímajúceho poštu pre našu doménu

@ IN	MX	10	mail.skola.internal
@ IN	MX	20	mail2.skola.internal
ucitel	MX		mail.skola.internal
student	MX		mail.skola.internal

- Záznam o dvoch mailových serveroch pre emaily, ktoré sa končia na skola.internal. Prioritu má ten s nižším číslom (mail.skola.internal). Ďalšie záznamy sú pre adresy, ktoré sa končia na ucitel.skola.internal alebo student.skola.internal.

Najčastejšie typy záznamov

- A – mapuje záznam na IPv4 adresu

@	IN	A	10.10.10.1
www	IN	A	10.10.10.1
mail	IN	A	10.10.10.2
proxy	IN	A	10.10.10.3
pc09	IN	A	10.10.10.109

Najčastejšie typy záznamov

- AAAA – mapuje záznam na IPv6 adresu

@	IN	AAAA	3ffe:80ee:1988::0001
www	IN	AAAA	3ffe:80ee:1988::0001
mail	IN	AAAA	3ffe:80ee:1988::0002

Najčastejšie typy záznamov

- CNAME – slúži na definíciu aliasov pre už existujúci A záznam (napr. ak sa nachádza na jednom serveri viac služieb a treba ich odlíšiť – www, db, mail, ...)

u	IN	CNAME www.skola.internal
s	IN	CNAME www.skola.internal
ftp	IN	CNAME mail.skola.internal

- Vytvoril som si záznam pre u.skola.internal, ktorý vráti IP adresu www.skola.internal, ftp.skola.internal vráti adresu mail.skola.internal
- Výhodou je, že ak sa zmení IP adresa servera, stačí zmeniť A záznam a netreba meniť aj množstvo záznamov v aliasoch

Vzor zónového záznamu

@ IN	SOA	skola.internal.	admin.skola.internal. { 64 3600 300 172800 43200 }
------	-----	-----------------	--

@	IN	NS	ns.skola.internal
@	IN	NS	ns.sanet.sk

@	IN	MX	10	mail.skola.internal
@	IN	MX	20	mail2.skola.internal
ucitel		MX		mail.skola.internal
student		MX		mail.skola.internal

@	IN	A	10.10.10.1
www	IN	A	10.10.10.1
mail	IN	A	10.10.10.2

@	IN	AAAA	3ffe:80ee:1988::0001
www	IN	AAAA	3ffe:80ee:1988::0001
mail	IN	AAAA	3ffe:80ee:1988::0002

ucitel	IN	CNAME	www.skola.internal
student	IN	CNAME	www.skola.internal
ftp	IN	CNAME	mail.skola.internal
intranet	IN	CNAME	mail.skola.internal

Primárny a sekundárny server

- Primárny DNS server spravuje lokálne záznamy domén, pre ktoré je autoritatívny.
- Správca primárneho servera pridávať, modifikovať alebo mazať zónové záznamy primárnej zóny na tomto serveri.
- Sekundárny server pre doménu číta záznamy z primárneho pomocou procesu nazývaného "zone transfer".
- Tieto záznamy sú ukladané ako read-only kópie a periodicky sú znova načítavané z primárneho servera, pričom tvoria sekundárnu zónu

Stub zóna

- Stub zóna obsahuje záznamy (odkazy) na iné DNS servre
- Umožňuje urýchliť proces vyhľadávania záznamov, pretože nie je potrebné kontaktovať nadradené (prípadne root) servery ale stub zóna povie, ktorý DNS kontaktovať pre získanie požadovaného záznamu
- Dáta v stub zóne sa dokážu dynamicky modifikovať pri zmene alebo pridaní DNS servera v doméne načítaním údajov z tzv. master servera

Dopredné vyhľadávanie

- Dopredné vyhľadávanie alebo forward lookup sme si už popísali
- Je to prevod doménového mena na IP adresy
- Deje sa tak hierarchickým prechádzaním domén rôznych úrovní a odkazovaním na autoritatívne servery

Spätné (reverzné) vyhľadávanie

- Je prevod IP adresy na doménové meno
- Je to zložitý mechanizmus, proces podobný prehľadávaniu telefónneho zoznamu, keď na základe telefónneho čísla vyhľadávame meno
- Postupnosť prehľadávania však má zostať podobná

Spätné (reverzné) prehľadávanie

- Používa sa doména in-addr.arpa, ktorú si vytvoríme na serveri, kde chceme realizovať reverse lookup
- Pri dotaze píšeme požiadavku na zistenie mena pre danú IP adresu v obrátenom tvare
- Napríklad ak máme adresný priestor 147.232.42.0/24 bude zóna nazvaná ako 42.232.147.in-addr.arpa, pričom v nej bude záznam: 21 IN PTR www.spseke.sk

DNS Forwarding

- Ak potrebujeme, aby náš server odpovedal aj na dotazy na záznamy, ktoré nemá vo svojom zónovom súbore, musíme použiť DNS forwarder
- Pri konfigurácii povieme nášmu DNS serveru, aby sa na ďalšie záznamy pýtal iného DNS servera, ktorého IP adresu mu uvedieme v konfigurácii
- Defaultné nastavenie je také, že ak neexistuje DNS forwarder, budú sa všetky dotazy na záznamy odosielať na root DNS servery

Podmienený DNS forwarding

- Ak máme dve navzájom odlišné domény, ktoré nie sú v spoločnej sieti a nie sú ani viditeľné z internetu (napr. interná AD doména) a potrebujeme aby si navzájom rozpoznávali názvy hostov, využijeme DNS podmienený (conditional) forwarding
- Pri konfigurácii conditional forwardingu zadáme podmienku (teda názov domény) a IP adresu DNS servera, na ktorú sa má preposlať požiadavka na zistenie príslušných údajov (napr. IP adresy)

Zdroj

- <http://www.fi.muni.cz/~kas/pv090/referaty/2013-jaro/dns.html>
- <http://www.ervin.sk/uvod-do-dns/>
- <http://www.samuraj-cz.com/clanek/dns-domain-name-system-zamereno-na-microsoft/>
- <http://www.youtube.com/watch?v=KjMDtIR6Mhk>
- [http://www.youtube.com/watch?v= GJPBg1D0sY](http://www.youtube.com/watch?v=GJPBg1D0sY)
- <http://www.youtube.com/watch?v=alumRsTngjl>