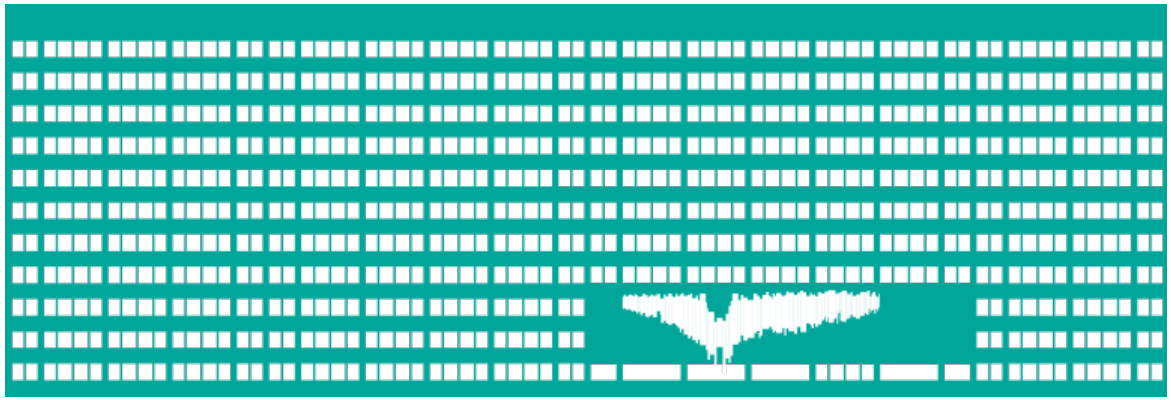
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

DNS



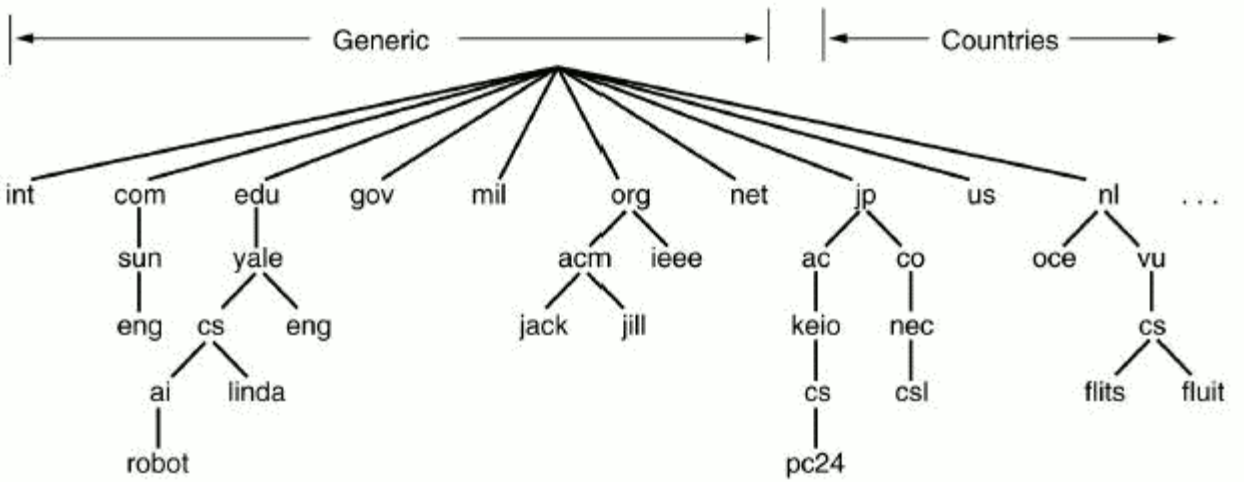
Počítačové sítě
11. cvičení

Úvod k DNS (Domain Name System)

- Jmenná služba používaná v Internetu
- Mapuje doménová jména na IP adresy a naopak
- Komunikace probíhá nad UDP (port 53), pro velké požadavky/odpovědi se používá TCP (port 53)
- DNS server zpracovává a odpovídá na požadavky od Resolveru.
- Resolver je komponenta systému, která komunikuje s DNS serverem

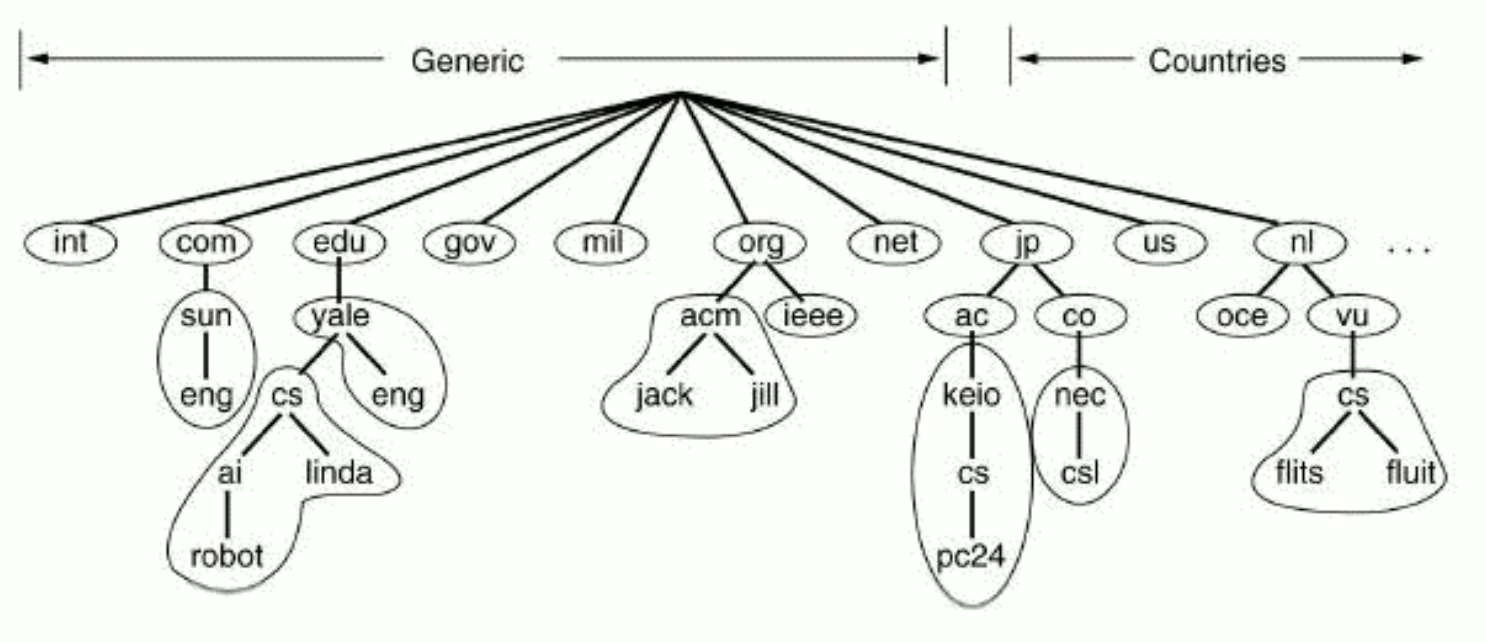
Domény

- Domény:
  - generické : .edu, .com, …
  - označení států : .cz, .it, .uk, …
- doménové jména mají hierarchickou strukturu (kořenem stromu je doména “.”)
- Maximální délka jména je 256 znaků (1 komponenta max. 63)



Zóna

- Zóna je část stromu uložená na jednom DNS serveru
- DNS server je autoritativní pro domény obsažené v jím spravované zóně



Typy záznamů v DNS

- **SOA** – *Start of authority* – vymezuje základní informace o doméně jako jsou hlavní nameserver, email správce a hodnoty expirací
- **NS** – *Name server* – označuje autoritativní servery příslušné domény
- **MX** – *Mail exchange* – označuje mail server, který má na starost doručování emailu do této domény
- **A** – Address – spojuje doménové jméno s IP adresou
- **CNAME** – *Canonical name* – přiřazuje alias k doménovému jménu
- **PTR** – *Pointer* – slouží k ukládání reverzních záznamů

Zjištění informací z DNS serveru – příkaz nslookup

- Alternativa programu **dig** pro OS Windows
- Ovládání pomocí příkazu nslookup.
- Příkazy:
  - **set type=**<*typ_záznamu*>
    - (NS,A, ... nebo ANY, který zobrazí všechny typy)
- Př:
  - C:\> **nslookup**
    > **server** DNS_server
    > **set type**=A
    > homel.vsb.cz
- Další nástroj – **host**

Zjištění informací z DNS serveru – příkaz dig

- Vyhledává a zobrazuje informace z DNS serveru (Linux)
- Parametry příkazu dig:
  - **@**<*server*> - jméno nebo IP adresa DNS serveru
  - **-t** <*typ záznamu*> - určujeme, o jaký typ záznamu máme zájem
  - **-p** <*port*> - pokud nepoužíváme standardní port
- Příklad: **dig -t A homel.vsb.cz** (nebo dig homel.vsb.cz A)
- Odpovědi DNS serveru na dotaz:
  - **QUESTION SECTION** – dotaz na DNS server
  - **ANSWER SECTION** – odpověď na dotaz
  - **AUTHORITY SECTION** – určuje, který DNS server je autoritou
  - **ADDITIONAL SECTION** – dodatečné informace. Většinou zobrazuje IP adresy DNS serverů, které jsou autoritou.

Příklady dotazů příkazu DIG

- Zobrazení IP adres pro yahoo.com
  - **dig** yahoo.com –t A nebo dig yahoo.com A
- Vrátí seznam mail serverů pro yahoo.com
  - **dig** yahoo.com MX +noall +answer
- Seznam name serverů, které jsou autoritou pro yahoo.com
  - **dig** yahoo.com NS +noall +answer
- Zobrazí vše co jsme zkoušely předešlými příkazy
  - **dig** yahoo.com ANY +noall +answer
- Zobrazení PTR záznamu pro reverzní překlad
  - **dig** 49.149.196.158.in-addr.arpa. ANY +noall +answer

Konfigurace DNS serveru BIND

- **Bind** je implementace DNS serveru pro OS Linux, Windows a FreeBSD. Konfigurace je rozdělena v několika souborech.
- `/etc/bind/`**`named.conf`** – hlavní konfigurační soubor. Zde jsou definovány zóny, pro které je server autoritativní nebo ostatní konfigurační soubory, které mají být načteny.
  - `options { // Nyní umísťováno do` **`named.conf.options`**
    `directory "/var/cache/bind";`
    `// v tomto adresáři hledá bind konfigurační soubory`
    `recursion yes;` `// povolit rekurzivní překlad +`
    `// Odkomentovat sekci forwarders a nastavit na` **`158.196.0.53`**
    `// Nefunguje-li aktuálně, nastavit dnssec-validation na` **`no`**
    `…`
    `};`

    `//V současných verzích BIND` **`named.conf.default-zones`**
    `zone "." {` `// odkaz na zónový soubor s kořenovými servery`
    `type hint;// hint znamená, že obsahuje pouze seznam root serverů`
    `file "/etc/bind/db.root";`
    `};`
- /etc/bind/db.* – definice záznamů pro danou zónu (např. db.testA)

Definice zóny testEB4x

- V distribuci **bind** najdeme implicitně předkonfigurované tři zóny (**localhost**, **127.in-addr.arpa**, **0.in-addr.arpa**)
  - Definice další zóny je znázorněna následující sekci souboru **named.conf.local** (nebo named.conf)
    - ```
      zone "testEB4x.cs.vsb.cz" {
      type master;  //tento name server bude
                    //primární a autoritativní
                    //pro tuto doménu.
      file "/etc/bind/db.testEB4x";
        //Soubor s definicí jednotlivých záznamu
      };
      ```
      ```

Konfigurace zóny testEB4 soubor db.testEB4

- **$ORIGIN cs.vsb.cz.**
  - Hodnota ORIGIN je implicitně vložena za jména v tomto souboru, která nekončí tečkou.
- **$TTL 604800**
  - implicitní doba udržování záznamu v cache
- Záznam **SOA** musí být **vždy** uveden **1x** na začátku zónového souboru:

```
testEB4x IN SOA  ns.testEB4x admintestEB4x.vsb.cz.
              (2018092414 ;
               604800 ;
               … )
```

- **ns.testEB4**
  - jméno primárního DNS serveru domény (ns.testEB4x.cs.vsb.cz.)
  - **admintestEB4.gmail.com.**
    - E-mail správce domény (místo @ se používá “.”)

Konfigurace zóny testEB4 soubor db.testEB4 (pokračuje)

- Hned za **SOA** záznamem by měl být **NS** záznam, určující DNS server pro danou doménu (`$ORIGIN testEB4x.cs.vsb.cz.`)

```
                NS          a.ns
        a.ns    A           158.196.246.234
```

- Přiřazení IP adresy k jménu pc1.testEB4x.cs.vsb.cz.

```
        pc1                 A     158.196.246.20
                            TXT   "pocitac c.1"
```

- Definice aliasu pro pc1

```
        www                 CNAME       pc1
```

- Vazební NS záznam

```
        poddom              NS    a.ns.poddom
        a.ns.poddom         A     158.196.246.20
```

Konfigurace DNS serveru pro reverzní překlad

- Reverzní překlad slouží pro mapování IP adres na doménová jména
- Definice zóny pro reverzní překlad vložíme do souboru **named.conf.local** (dříve přímo v named.conf)
- Doménové jméno pro záznam k reverznímu překladu adresy A.B.C.D je
  D.C.B.A.in-addr.arpa.
  - ```
    zone "135.196.158.in-addr.arpa" {
     type master;
     file "/etc/bind/db.135.196.158.in-addr.arpa";
    };
    ```
    ```

Konfigurace zóny 135.196.158.in-addr.arpa.

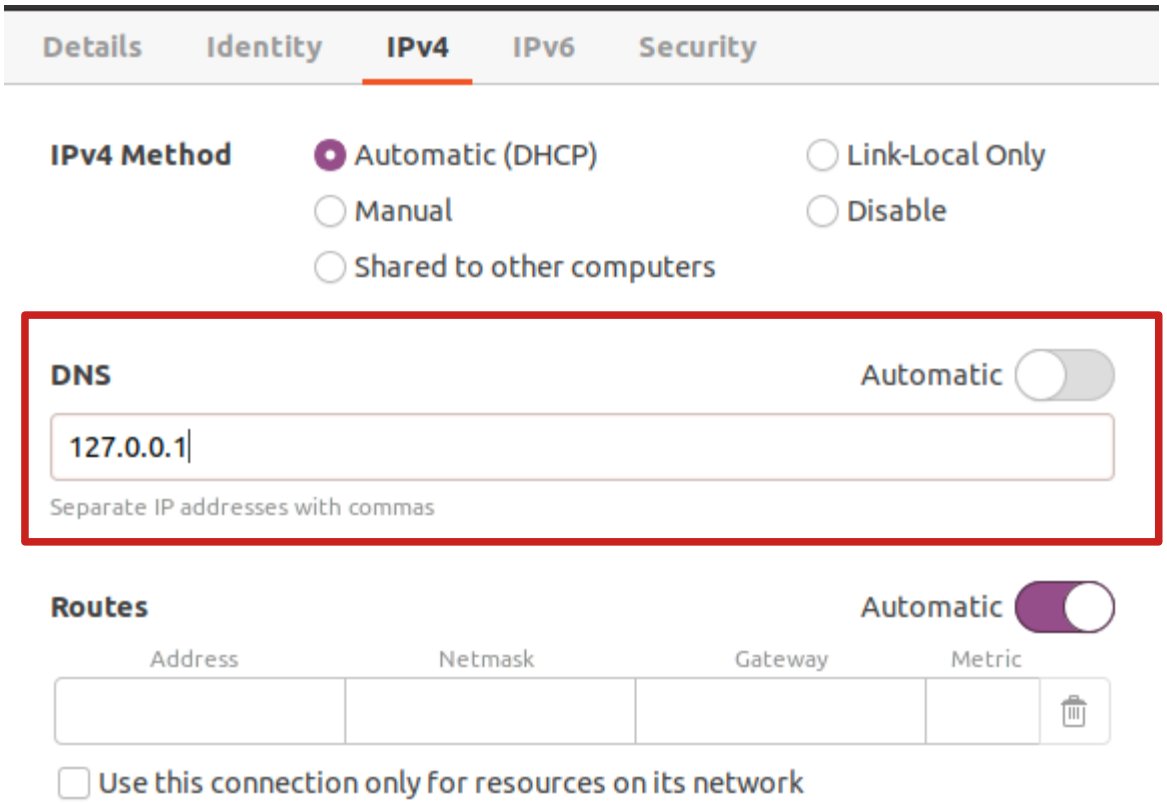
- Platí zde stejné pravidla jako při definici normální zóny. Musí existovat záznam typu **SOA** a **NS** (name server zodpovědný za doménu)
- Místo **A** záznamu použijeme záznam **PTR**, který mapuje IP adresy na doménová jména

```
$ORIGIN 135.196.158.in-addr.arpa.
66          PTR pc1.testEB4x.cs.vsb.cz.
```

resolv.conf, hosts, host.conf

- Soubory, obsahující konfiguraci **resolveru** (Linux), v **/etc**
  - **resolv.conf** – konfigurace DNS na straně klienta
    - Konfigurační příkazy:
      - search <doména> – implicitní doplňovaná doména
      - nameserver <IP adresa DNS serveru>
  - **hosts** – ručně (staticky) nastavené adresy (i ve Windows)
    - <IP adresa> <jméno> [<jméno2> ...]
  - **host.conf** – pořadí statických a DNS adres při resolvingu (ignorováno v novějších OS)
    - order hosts, bind – nejprve soubor hosts, při neúspěchu DNS

Změna nastavení rekurzivního DNS serveru v GUI



Současný resolver systemd-resolve na Ubuntu 20.04

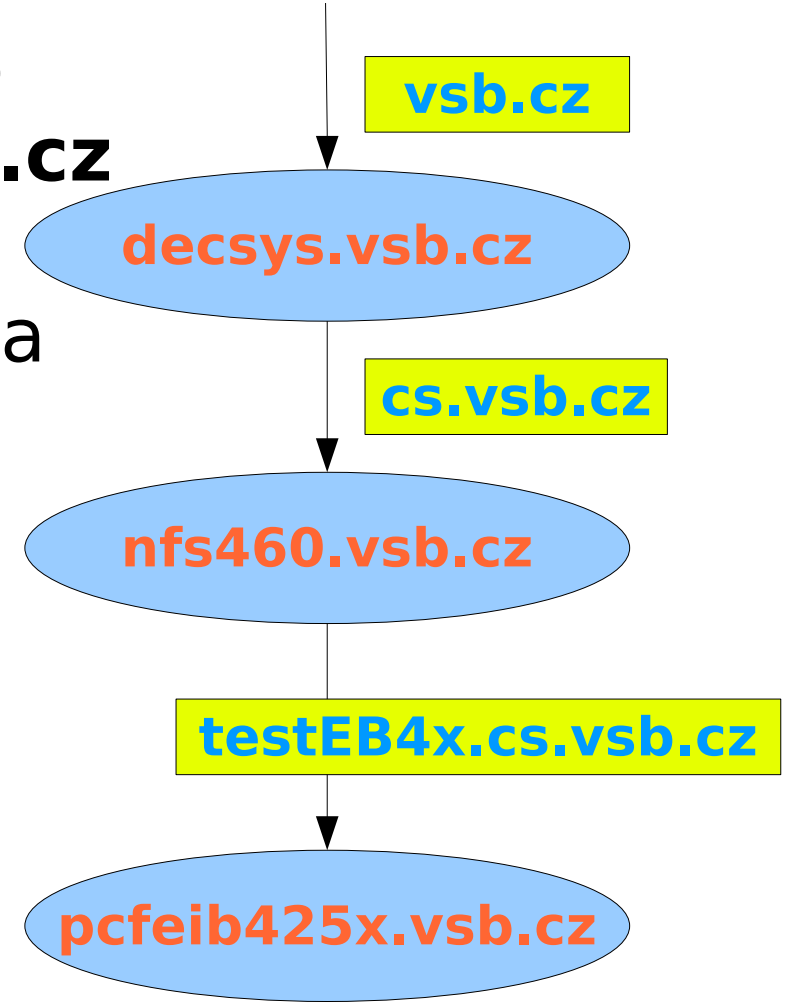
- Má vlastní rekurzivní kešující server, běžící na IP adrese 127.0.0.53 a přepisuje resolv.conf
- Lze zobrazit jeho stav pomocí **systemd-resolve --status**
- Přepisuje /etc/resolve.conf, proto není vhodné jej měnit ručně (DHCP klient jej může přepsat)
- Lze změnit server, který má kontaktovat na lokální pomocí
  **systemd-resolve –set-dns=<IP_počítače> **
  --set-domain=<zóna> --interface=eth*0*
- Mezipaměť systemd-resolve lze smazat pomocí **systemd-resolve --flush-caches**

Nástroje pro testování konfigurace DNS serveru

- Kontrola konfiguračních souborů
  - **named-checkconf** */etc/bind/named.conf*
    - Popř. individuální soubory s konfigurací
  - **named-checkzone** *zóna db_soubor_zóny*
    - Out-of-zone data nebo chybějící A záznamy pro domény, kde se opakuje část DN → chyba
- Spuštění DNS serveru v popředí (sudo)
  - **named -g**
  - Nelze-li spustit, zkusit **service bind9 stop**

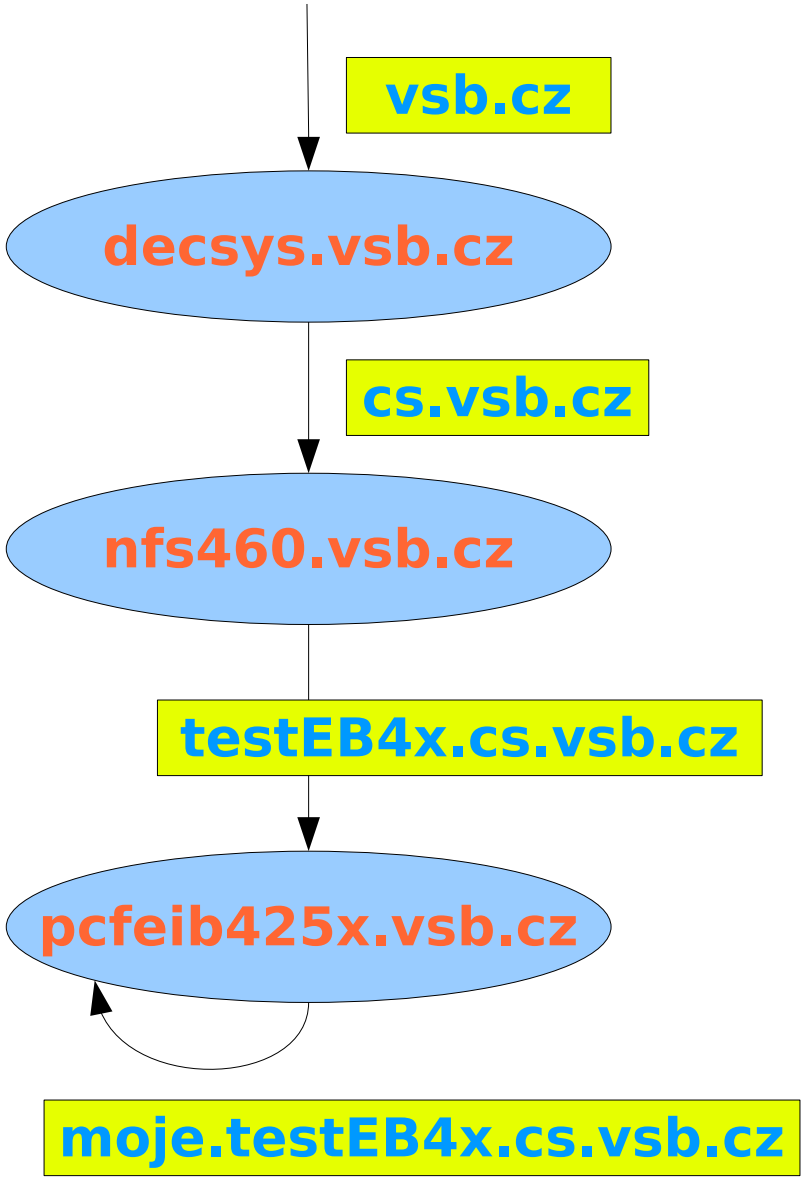
Úloha č.1

- Konfigurace name serveru bind.
  - Připojení DNS serveru pro doménu testEB4x**.cs.vsb.cz** do stromu
  - Vložení záznamu **SOA**, **A** a **TXT**
  - Nastavení rekurzivního překladu
  - Nastavení klienta (**`/etc/resolv.conf`**)
  - Otestování



Úloha č.2

- Připojení další úrovně (poddomény) do DNS serveru vytvořeného v předchozí úloze.
- Vložte záznam typu **SOA** a potřebné **NS** a **A** záznamy, pro poddoménu a také záznamy **MX** a **TXT**.



Úloha č.3

- Nakonfigurujte DNS server, aby byl autoritativním pro doménu **X.Y.Z.in-addr.arpa**, kde Z.Y.X je cvičícím přidělený prefix adres třídy C.
- Do této domény vložte záznam typu **PTR** pro nějakou IP adresu
- Ověřte funkčnost reverzního překladu.
- Klienta ověřujícího funkčnost nasměrujte přímo na váš DNS server.