DNS

DNS

Poznáváte tyto systémy?

146.102.16.4
146.102.14.10
146.102.20.10
146.102.18.43

194.48.241.132
90.183.101.70
80.95.112.246
185.15.59.224

2001:718:1:1f:50:56ff:feee:46

DNS

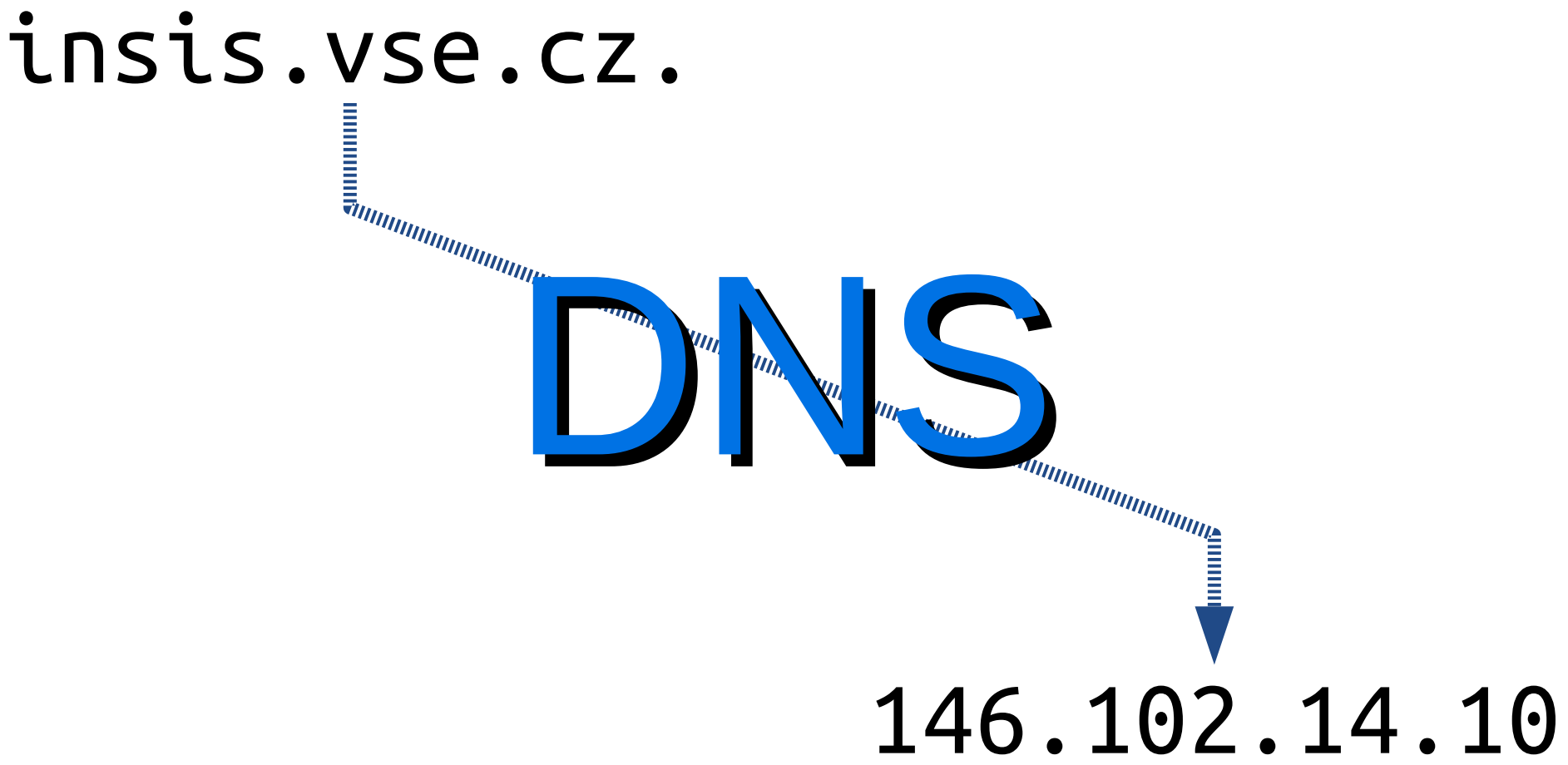
Poznáváte tyto systémy?

www.vse.cz	czso.cz
insis.vse.cz	chmi.cz
moodle.vse.cz	sujb.cz
4iz110.vse.cz	wikipedia.org

cesnet.cz

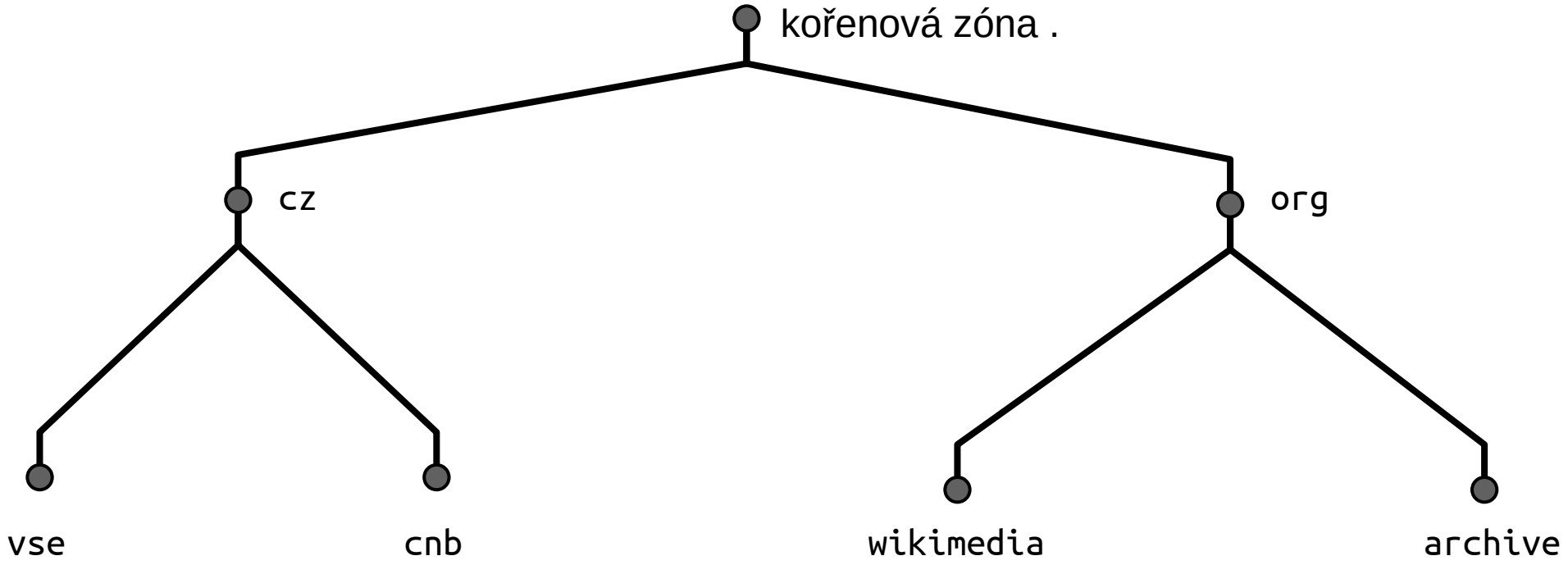
DNS

- chci-li komunikovat s nějakým systémem v internetu, musím znát jeho **IP adresu**
- zbytek zařídí směrovače (routery)
- ale IP adresy se špatně pamatují (IPv4 i IPv6)
- **jména** si člověk pamatuje lépe
- **D**omain **N**ame **S**ystem (DNS) je **distribuovaný**, **hierarchický** systém, který nám *mimo jiné* převádí **jména** (domény) na **adresy** (IP)


insis.vse.cz.
DNS
146.102.14.10

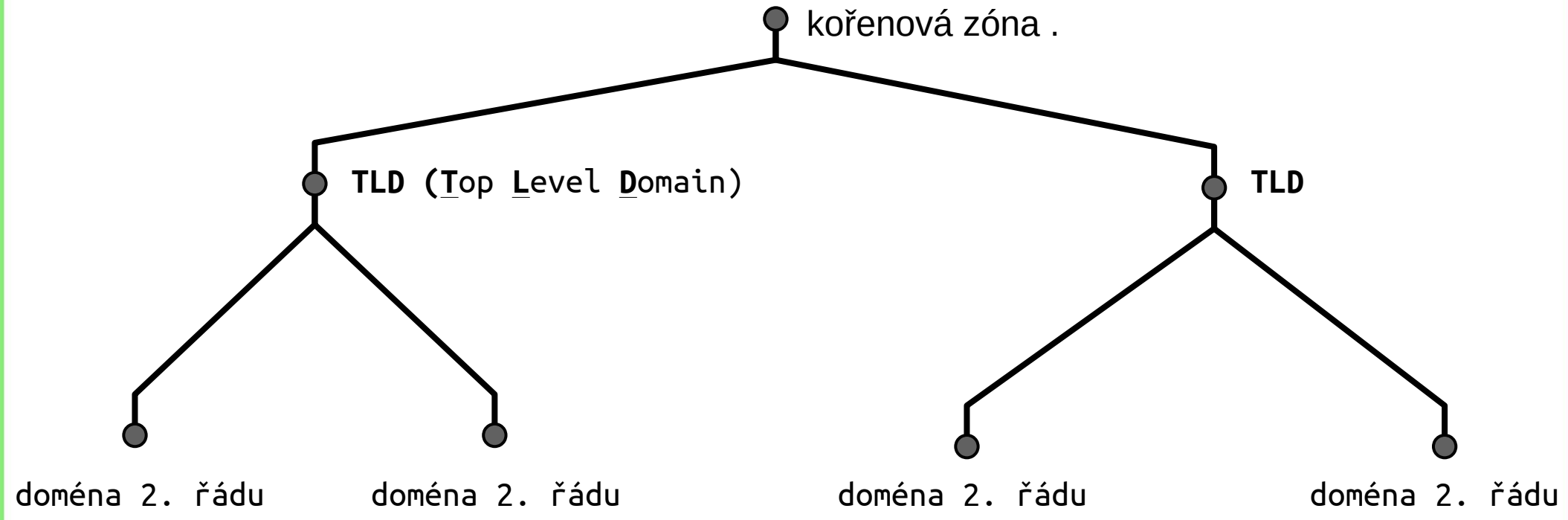
Domain Name System

- **hierarchický systém** doménových jmen



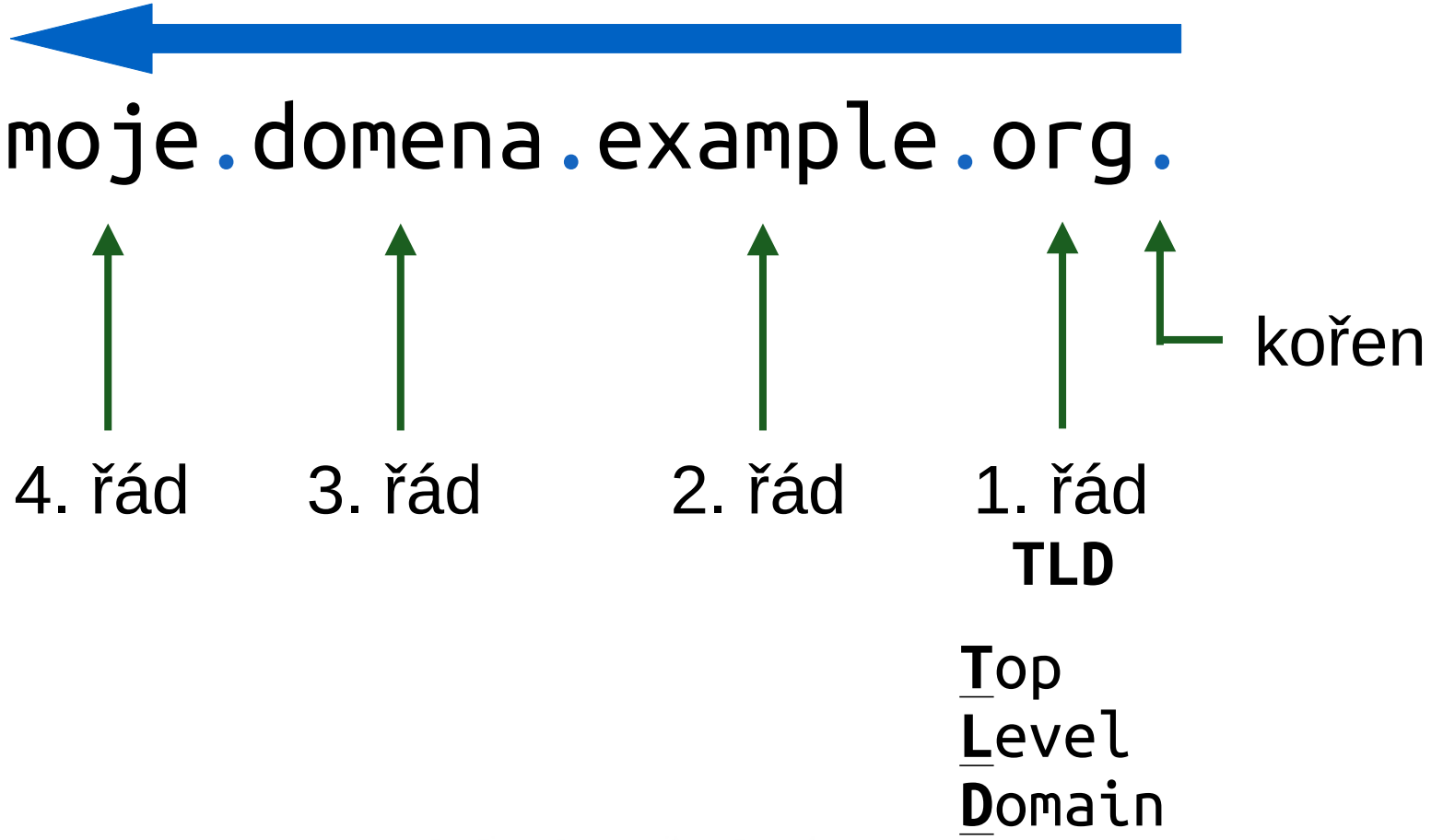
Domain Name System

- **hierarchický systém** doménových jmen



Doména

- hierarchický systém **doménových jmen**



DNS

- převod textových jmen na adresy je starší než TCP/IP *(druhá polovina 70. let)*
  - využívalo se souborů `hosts.txt` a podobných

    `146.102.18.43 4iz110.vse.cz 4iz110`
  - `/etc/hosts` v Unixových systémech se používal už za ARPANETu (předchůdce internetu) v 70. letech!
- DNS bylo zřízeno *až* v roce **1983** a v roce **1987** bylo inovováno (**RFC 1034**, **RFC 1035**)
- DNS má podobu **distribuované databáze**, kde jsou DNS **záznamy** uloženy v **zónách** na mnoha různých *autoritativních* **DNS serverech**

DNS

- **DNS strom** je administrativně dělen do **zón**, přičemž každá *zóna* je *uložena* a *spravována* na konkrétním (*autoritativním*) **DNS serveru** (zpravidla je jich více)
- např. doména `vse.cz` používá tyto DNS servery:

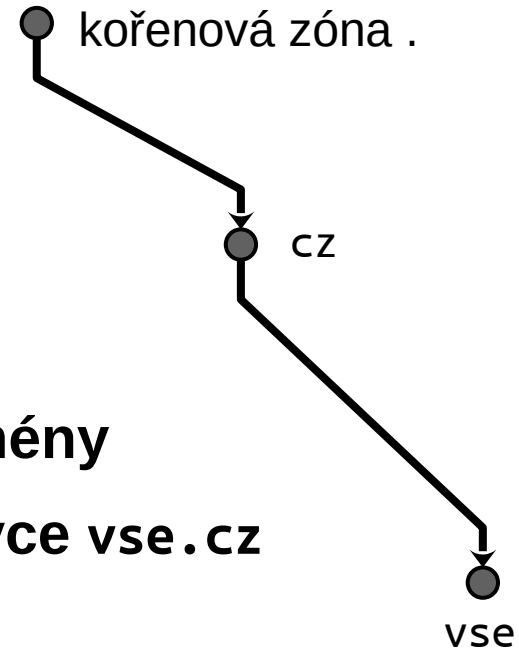
```
vse.cz.    IN    NS    ns2.vse.cz.
vse.cz.    IN    NS    mx2.vse.cz.
vse.cz.    IN    NS    ns1.vse.cz.
```

- **DNS zóna** může zahrnovat více **subdomén**
  - subdoména je doménové jméno **vyššího** řádu, tzn. pro doménu **`vse.cz.`** jsou **`insis.vse.cz.`** nebo **`4iz110.vse.cz.`** subdomény
- **DNS server** může obsahovat/obsluhovat více **zón**

DNS

- servery výše v hierachii DNS **delegují** správu nad konkrétní doménou prostřednictvím **odkazu** na DNS server, kde je spravována příslušná zóna
- **odkaz** má podobu **`NS`** záznamu

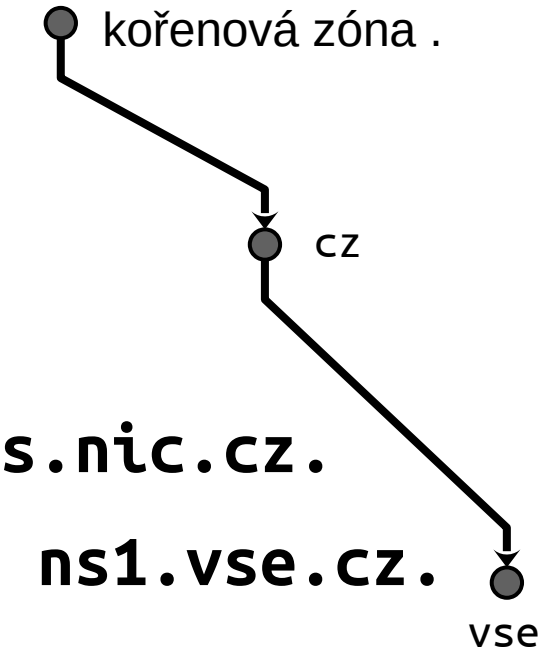
  (NS = **N**ame **S**erver)
- příklad: doména `vse.cz`
  - **kořenový NS** odkazuje na **NS správce `.cz` domény**
  - **NS správce `.cz` domény** odkazuje na **NS správce `vse.cz`**



DNS

- servery výše v hierachii DNS **delegují** správu nad konkrétní doménou prostřednictvím **odkazu** na DNS server, kde je spravována příslušná zóna
- **odkaz** má podobu **`NS`** záznamu

  (NS = **N**ame **S**erver)
- příklad: doména `vse.cz`
  - kořenový server: **`cz.`** `IN NS` **`a.ns.nic.cz.`**
  - server `a.ns.nic.cz`: **`vse.cz.`** `IN NS` **`ns1.vse.cz.`**



Kořenová zóna

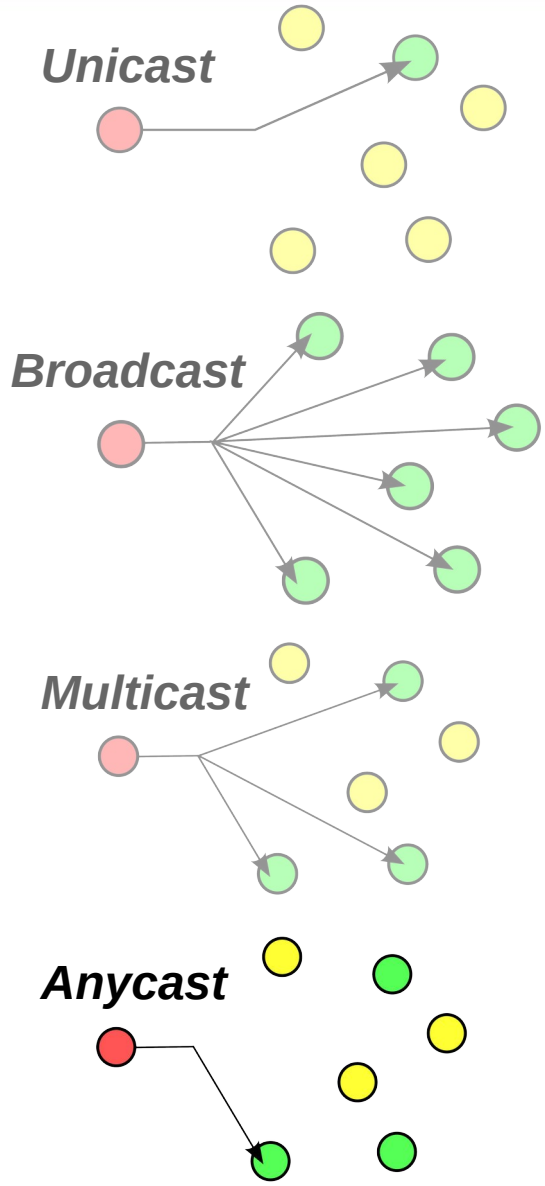
- kořenová zóna je *bezejmenná* zóna, která tvoří počátek DNS stromu
  - je uložena na **13** kořenových DNS autoritách

```
a.root-servers.net   198.41.0.4,      2001:503:ba3e::2:30
b.root-servers.net   170.247.170.2,   2801:1b8:10::b
...
m.root-servers.net   202.12.27.33,    2001:dc3::35
```

  - spravují je **různé subjekty** (od ICANN po komerční subjekty jako *Verisign, Inc.*, apod.)
  - 13 autorit má po světě rozmístěno **stovky fyzických serverů** (*replik*), na které je směrován provoz **anycast**em
  - kořenová zóna obsahuje **NS** záznamy pro **TLD**

Typy směrování

- *Unicast – jeden jednomu*
  - většina komunikace na internetu
- *Broadcast – jeden všem*
  - všesměrové vysílání
- *Multicast – jeden mnohým* či *mnozí mnohým*
  - oproti broadcastu se příjemci „*přihlašují*" k odběru
- **Anycast** – jeden jednomu z mnoha
  - více serverů, vybere se jeden, zpravidla ten geograficky nejblíže
  - např. kořenové DNS servery



DNS zóna

konkrétní část jmenného prostoru DNS stromu spravovaná daným správcem

- *např. konkrétní doména druhého řádu (*`vse.cz`*)*
- **zóna** obsahuje sadu **DNS záznamů**
- **DNS záznam** představuje textovou informaci

```
4iz110.vse.cz.  IN   A   146.102.18.43
```

- existují různé typy DNS záznamů (dle typu uložené informace)
  - **SOA**, **A**, **AAAA**, **MX**, **CNAME**, **PTR**, **RRSIG**, **SRV**, **TLSA**, **TXT** a další

DNS infrastruktura

Typy DNS serverů

Michal Pečenka

DNS infrastruktura

- **Autoritativní** DNS servery
  - tvoří DNS strom
- **Rekurzory** (cachovací servery)
  - řeší DNS dotazy vyhledáváním mezi autoritativními servery
  - chvíli si pamatují odpovědi
- **DNS resolver**
  - služba OS (součást síťového stacku), prostřednictvím které si aplikace nechávají zodpovídat DNS dotazy
  - má nakonfigurované rekurzory (zpravidla od ISP), které používá k řešení DNS dotazů

Autoritativní name servery

- autoritativní name servery tvoří **DNS strom**
- jsou v nich **permanentně uložené** všechny zóny a DNS záznamy (nositelé zón/záznamů)
- **odpovídají** na dotazy **rekurzivních** serverů
- autorita je **delegována** z autoritativních serverů výše položených v hierarchii DNS
  - delegování je realizováno **pomocí NS záznamů**
- autoritativní servery se dělí dle funkčnosti na **primární** a **sekundární**

Autoritativní name servery

- **primární** - primární zdroj dat a bod pro správu (a případné změny) záznamů v zóně
- **sekundární** - pomocí přenosu zóny (*zone transfer*) si sekundární name server stahuje zóny z primárního (automatizované kopie primárního)
  - těmito staženými daty pak odpovídá na DNS dotazy rekurzorů
  - zóny se na sekundárních serverech nemodifikují
  - stahování a servírování dat se řídí **SOA** záznamem (konfigurují se prostřednictvím samotného DNS)

Start **O**f **A**uthority (SOA záznam)

```
cnb.cz.  1800  IN SOA  tm0.cnb.cz. hostmaster.cnb.cz.
1707316111 14400 3600 2419200 1200
```

Start Of Authority (SOA záznam)

```
cnb.cz.  1800  IN SOA  tm0.cnb.cz. hostmaster.cnb.cz.
1707316111 14400 3600 2419200 1200
```

1800 – **TTL SOA** záznamu (v sekundách)

tm0.cnb.cz. – **primární name server** domény

hostmaster.cnb.cz. – **mail správce zóny** (první tečka = zavináč)

Start Of Authority (SOA záznam)

```
cnb.cz.  1800  IN SOA  tm0.cnb.cz. hostmaster.cnb.cz.
1707316111 14400 3600 2419200 1200
```

1707316111 – **sériové číslo** – **číslo revize zóny** – povýší-li, sekundární NS spustí *zone transfer* a stáhne si zónu z prim. NS

14400 – **refresh** – jak často se má sekundární NS dotazovat na *sériové číslo* ze **SOA** primárního NS, aby zjistil, zda-li nepovýšilo

3600 – **retry** – za jak dlouho má sekundární NS zkoušet znovu kontaktovat primární NS, pakliže se mu to nepovedlo

2419200 – **expire** – pokud primární NS po této lhůtě neodpověděl, sekundární NS přestane odpovídat na dotazy k této zóně

1200 – **TTL** – původně minimální TTL, pak výchozí TTL, dnes TTL pro **negativní caching** (uchovávání informace, že záznam neexistuje)

Rekurzory = cachovací servery

- **rekurzivně vyhledávají** v autoritativních serverech DNS stromu a **cachují** odpovědi dle TTL záznamů
  - musí znát kořenové DNS servery (**root servery**)
  - ty je odkáží na další jmenné servery v DNS stromu, a rekurzory tak **postupně vyhledávají** požadovanou informaci pokládáním dalších a dalších DNS dotazů, dokud se nedostanou k cíli *(rekurzivní vyhledávání)*
  - získanou **odpověď** si **uloží do cache** a na další dotaz vrátí cachovanou informaci
  - po vypršení **TTL** záznamu záznam z cache mizí a rekurzor opět provede rekurzivní vyhledávání
- ISP zpravidla nabízí svoje rekurzory klientům (typicky přes DHCP)

Příklad řešení dotazu

- **Rekurzor**: Ahoj **root server**e, hledám **A**dresu ke jménu **`isis.vse.cz`**
- **Root server**: To sice nevím, ale zkus se zeptat **`NS`** serverů domény **`cz`**:

```
cz.                     172800  IN      NS      a.ns.nic.cz.
cz.                     172800  IN      NS      b.ns.nic.cz.
cz.                     172800  IN      NS      c.ns.nic.cz.
cz.                     172800  IN      NS      d.ns.nic.cz.
```

- **Rekurzor**: Ahoj **cz server**e, hledám **A**dresu ke jménu **`isis.vse.cz`**
- **cz server**: To sice nevím, ale zkus se zeptat **`NS`** serverů domény **`vse.cz`**:

```
vse.cz.                 3600    IN      NS      mx2.vse.cz.
vse.cz.                 3600    IN      NS      ns1.vse.cz.
vse.cz.                 3600    IN      NS      ns2.vse.cz.
```

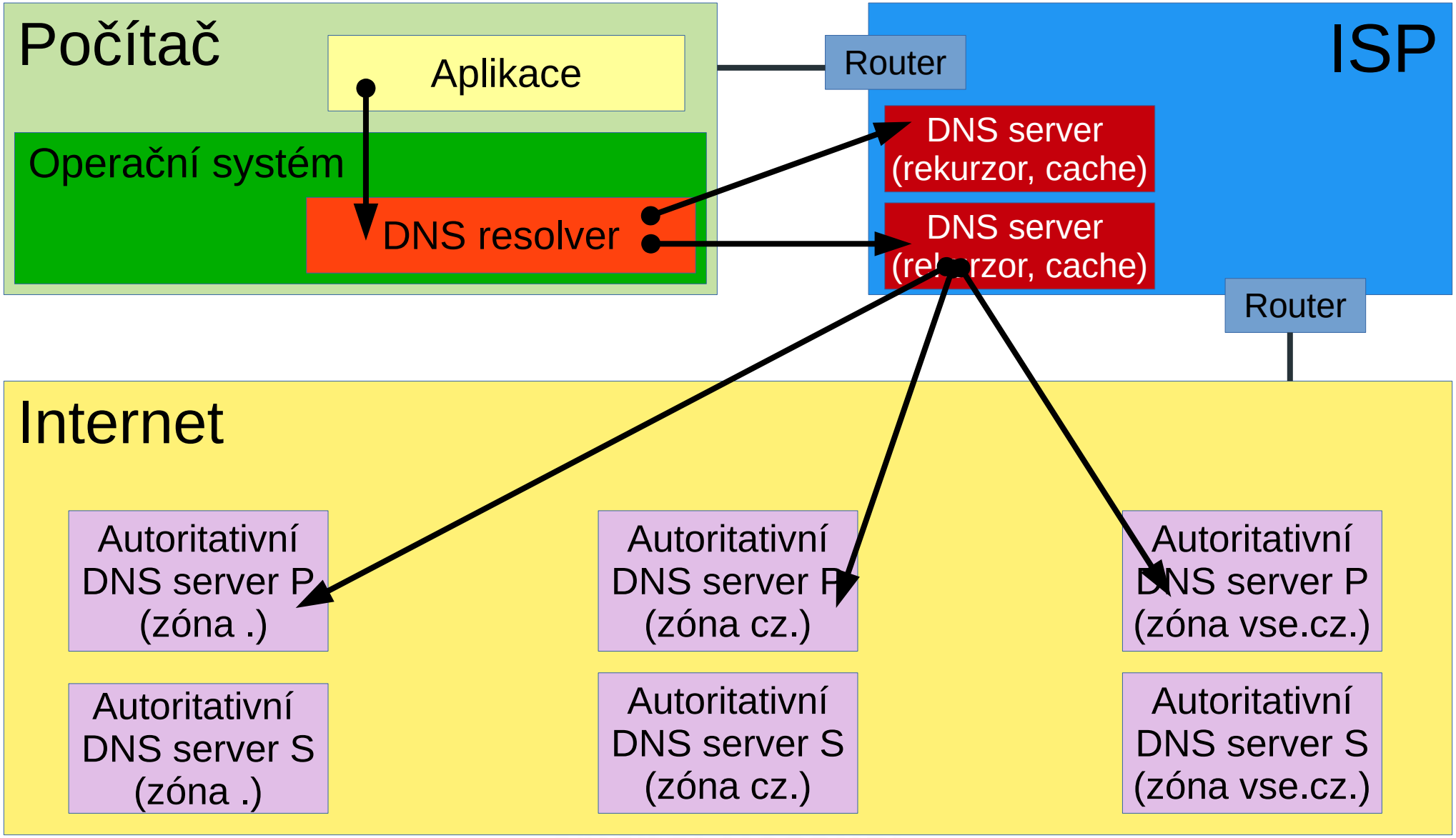
- **Rekurzor**: Ahoj **vse server**e, hledám **A**dresu ke jménu **`isis.vse.cz`**
- **vse.cz server**: **A**dresa ke jménu **`insis.vse.cz`** je **`146.102.14.10`**

```
isis.vse.cz.            7200    IN      A       146.102.14.10
```

DNS Resolver

- **služba OS**, která bývá součástí síťového stacku, ale existují i samostatné implementace
- má nastaveny **rekurzory** (1-2, zpravidla od ISP)
  - *Linux*: servery jsou nastavené v `/etc/resolv.conf`
  - `/etc/hosts` stále funguje (dokonce i ve Windows)
- **aplikace** využívají resolver a pokládají DNS dotazy jemu
  - *Linux*: `getaddrinfo()` céčkové knihovny (`libc`)
- resolver **přeposílá** dotazy rekurzorům
- odpovědi se vrací aplikaci a cachují (*Linux*: `nscd`)

Princip fungování DNS resolveru



DNS protokol

DNS záznamy

Michal Ďačeľak

DNS protokol

- od **1983**, RFC **1034**, **1035** a pak mnoho dalších
- DNS využívá 2 typy zpráv: **dotaz** (*query*) a **odpověď** (*response*)
- **DNS zpráva** obsahuje **hlavičku** a čtyři **sekce** obsahu: dotaz (question), odpověď (answer), autorita (authority) a doplňkový prostor (additional)
- aplikační protokol DNS využívá port **53** **TCP** i **UDP**
  - výchozí volba: **UDP** (1 paket dotaz, 1 paket odpověď)
  - volitelně lze použít **TCP** pro *dotaz*, *odpověď* nebo ***zone transfer***

DNS záznam

DNS záznam = **R**esource **R**ecord obsahuje:

- **`NAME`** – k jakému doménovému jménu se záznam vztahuje
- **`TYPE`** – typ záznamu (`A`, `AAAA`, `SOA`, `NS`, `MX`, apod.)
- **`CLASS`** – třída* záznamu (typicky **`IN`** = Internet)
- **`TTL`** – time to live daného záznamu v cache
- **`RDATA`** – data záznamu (jeho obsah)

NAME	TTL	CLASS	TYPE	RDATA
vse.vse.cz.	7206	IN	A	146.102.16.2
sujb.cz.	86400	IN	MX	10 hornet.erc-cr.cz.

**) třída záznamu umožňuje vytvářet v DNS nezávislé jmenné prostory, kde každá třída může mít úplně jiné záznamy, včetně NS, tedy i jinou delegaci autority*

Typy DNS záznamů

- **SOA** – autoritativní informace o doméně
- **A**, **AAAA** – IP **A**dresa
- **CNAME** – jmenný alias, odkaz na jiné jméno
- **MX** (**M**ail e**X**change) – poštovní server domény
- **TXT** – text (+ řada typů záznamů, které nejsou součástí standardu DNS)
- **NS** (**N**ame**S**erver) – odkaz na jiný DNS server
- **PTR** – (**P**oin**T**e**R**) – reverzní záznam
- a další (**RRSIG**, **SRV**, **TLSA**, apod.)

A a **AAAA** záznam

Překlad *doménového jména* na *IP **A**dresu*

A = IPv4 adresa (32 bitů)

AAAA = IPv6 adresa (128 bitů = 32 x **4** → 4x**A**)

Příklady A a AAAA záznamů:

Doménové jméno	*TTL*	*Třída*	*Typ*	*IP adresa*
webhosting.vse.cz.	7200	IN	**A**	**146.102.17.31**
chmi.cz.	1800	IN	**A**	**90.183.101.70**
jiri.peterka.cz.	3600	IN	**A**	**31.15.10.5**
icann.org.	3600	IN	**A**	**192.0.43.7**
icann.org.	3600	IN	**AAAA**	**2001:500:88:200::7**
4iz110.vse.cz.	7211	IN	**AAAA**	**2001:718:1e02:18::43**

CNAME záznam

CNAME (**C**anonical **NAME**) – alias, doménové jméno odkazující na jiné doménové jméno

- Hledá-li rekurzor jiný typ záznamu a narazí na CNAME, zopakuje dotaz se jménem uvedeným v CNAME

Příklady CNAME záznamu:

```
www.tul.cz.     1200   IN   CNAME   novy.tul.cz.
kizi.vse.cz.    7200   IN   CNAME   webhosting.vse.cz.
ci.vse.cz.      7200   IN   CNAME   webhosting.vse.cz.
```

směr odkazu

Příklad užití:

```
insis.vse.cz.   7211   IN   CNAME   isis.vse.cz.
isis.vse.cz.    7200   IN   A       146.102.14.10
```

MX záznam

MX (Mail eXchange) – **poštovní server** pro danou doménu (může jich být více) a jeho **priorita**

- **priorita** je číslo, kde platí inverzní vztah: vyšší číslo představuje nižší prioritu a naopak

```
czso.cz.   300   IN   MX    50 smtp3.czso.cz.
czso.cz.   300   IN   MX   300 mspool.gts.cz.
```

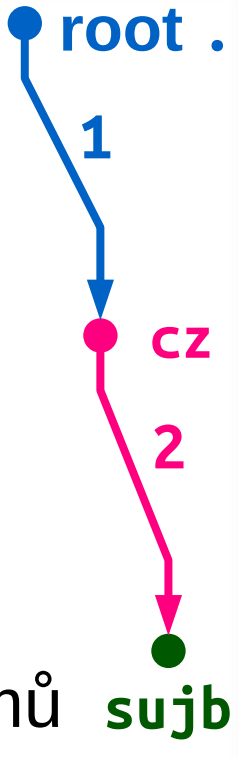
- poštovní (SMTP) server doručuje mail nejprve na server uvedený v **MX** záznamu o **nejvyšší** prioritě, v případě nezdaru zkusí **další v pořadí**

docm01@**vse.cz**

MX záznam

NS záznam

NS (**N**ame **S**erver) – odkaz na jiný DNS server



- NS záznamy slouží nejčastěji k **delegování autority** nad daným **doménovým jménem** na příslušný autoritativní **DNS server** správce domény:

```
1: cz.      172800  IN  NS  a.ns.nic.cz.
2: sujb.cz.  3600   IN  NS  ns.suro.cz.
```

- autoritativní NS výše v hierarchii deleguje autoritu nad doménou níže v hierarchii odkazem v podobě NS záznamů odkazujících na autoritativní NS správce domény
- každá doména má své autoritativní DNS servery uložené v NS záznamech:

```
chmi.cz.  3600  IN  NS  ns1.chmi.cz.
chmi.cz.  3600  IN  NS  ns2.chmi.cz.
```

PTR záznam

PTR (**P**oin**T**e**R**) záznam – reverzní záznam

- opak **A** záznamu, **PTR** záznam umožňuje zjistit jméno k **IPv4** nebo **IPv6** adrese

```
43.18.102.146.in-addr.arpa.  7211 IN PTR  4iz110.vse.cz.
246.112.95.80.in-addr.arpa. 86400 IN PTR  www.sujb.cz.
```

  IPv4 adresy se zadávají jako doménová jména v opačném pořadí oktetů, a to ve jmenném prostoru servisní domény **in-addr.arpa.**

- **PTR** záznamy nastavuje **vlastník IP adresy**
- **A** záznamy nastavuje **vlastník doménového jména**

PTR záznam

PTR (**P**oin**T**e**R**) záznam – reverzní záznam

- pro **IPv6** adresy se používá servisní doména **ip6.arpa.**

```
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.e.1.8.
1.7.0.1.0.0.2.ip6.arpa. 3862 IN PTR vse.vse.cz.
```

- **A/AAAA** a **PTR** záznamy jsou oddělené systémy s odlišnou autoritou (vlastník **domény** vs vlastník **IP adresy**), nesoulad je tedy častý:

```
nukib.cz.                          300 IN A   81.95.110.57
57.110.95.81.in-addr.arpa. 86400 IN PTR ds161.active24.cz.
```

PTR záznam

PTR (**P**oin**T**e**R**) záznam – reverzní záznam

- soulad mezi **A** a **PTR** záznamem se bere jako jistý test legitimity v případě antispamových řešení (nesoulad je penalizován či se stává důvodem k odmítnutí mailu)

```
vse.vse.cz.                  2427 IN A   146.102.16.2
2.16.102.146.in-addr.arpa. 794 IN PTR vse.vse.cz.
```

TXT záznam

TXT (Te**XT**) – textová informace uložená v DNS

```
cnb.cz.   3600  IN TXT "v=spf1 mx ip4:193.86.31.131
ip4:193.86.31.132 ip4:193.85.3.250 ip4:193.86.31.141
ip4:193.86.31.142 -all"
```

- příklady použití
  - ověření vlastnictví domény
    - služba vygeneruje nějaký dlouhý string, uživatel ho uloží jako `TXT` záznam do DNS, dotazem na `TXT` záznam služba ověří, že dotyčný je opravdu vlastník domény
  - konfigurace některých antispamových opatření (SPF, DKIM, DMARC)

SRV záznam

pro zajímavost

SRV (**S**e**RV**ice) – definice poskytované služby

```
    _service._proto.name     TTL  class SRV prio weight port target
 _xmpp-client._tcp.prales.eu. 6400 IN    SRV  5    0      5222 prales.eu.
_xmpps-client._tcp.prales.eu. 6400 IN    SRV  5    0      5223 prales.eu.
 _xmpp-server._tcp.prales.eu. 6400 IN    SRV  5    0      5269 prales.eu.
```

- RFC 2782, definuje umístění služeb (hostname serverů, protokoly a porty pro poskytovanou službu)
- využívají některé aplikační protokoly (SIP, XMPP, atd.)

AXFR dotaz (přenos zóny)

pro zajímavost

AXFR – autoritativní přenos zóny

- přenos celého zónového souboru
- pseudozáznam → není skutečným DNS záznamem (Resource Record), ale přenos zóny je iniciován standardním DNS dotazem typu AXFR
- používá se TCP, přístup pro transfer je často omezen jen na sekundární servery
- IXFR – inkrementální přenos (změny od posledního přenosu)

Nástroje pro diagnostiku DNS

Michal Začalka

Nástroje pro diagnostiku DNS

- Nástroje pro příkazovou řádku:
  - `Microsoft:` `nslookup`
  - `Unix:` **`dig`**`, drill, nslookup, host, delv`
- Omezení DNS provozu na VŠE
  - studentské stanice nemají možnost pokládat DNS dotazy jiným NS než rekurzorům VŠE
  - `4iz110.vse.cz` toto omezení (alespoň zatím) nemá

dig

- chceme-li jen pokládat dotazy rekurzoru:
  - `dig typ_záznamu doménové_jméno`
  - příklad: **`dig mx cnb.cz`**
- chceme-li pokládat dotazy konkrétnímu NS:
  - `dig @server typ_záznamu doménové_jméno`
  - příklad: **`dig @ns1.vse.cz soa vse.cz`**
- chceme-li krátký výpis: `+short`
  - příklad: **`dig +short mx cnb.cz`**

dig, drill a delv

- další zajímavé volby digu:

+dnssec	zažádá o DNSSEC záznamy
+trace	trasování dotazu (od root ns)
-4	použít jen IPv4
-6	použít jen IPv6

- **drill** je skoro totéž jako dig

-D	zažádá o DNSSEC záznamy
-T	trasování dotazu (od root ns)
-4 a **-6**	funguje jako u digu

- nástroj **delv** validuje DNSSEC
  - příklad: **delv mx cnb.cz**

Simulace řešení DNS dotazu
A záznam k www.cnb.cz

```
docm01@4iz110:~$ dig @k.root-servers.net a www.cnb.cz

;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57948
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; QUESTION SECTION:
;; www.cnb.cz.  IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
cz.     172800  IN      NS      a.ns.nic.cz.
cz.     172800  IN      NS      b.ns.nic.cz.

;; ADDITIONAL SECTION:
a.ns.nic.cz.    172800  IN      A       194.0.12.1
b.ns.nic.cz.    172800  IN      A       194.0.13.1

;; Query time: 11 msec
;; SERVER: 193.0.14.129
;; WHEN: Mon Feb 26 12:33:06 2024
;; MSG SIZE  rcvd: 275
```

Simulace řešení DNS dotazu
A záznam k www.cnb.cz

```
docm01@4iz110:~$ dig @a.ns.nic.cz. a www.cnb.cz

;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 10033
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 4
;; QUESTION SECTION:
;; www.cnb.cz.  IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
cnb.cz. 3600    IN      NS      tm0.cnb.cz.
cnb.cz. 3600    IN      NS      tm1.cnb.cz.

;; ADDITIONAL SECTION:
tm0.cnb.cz.     3600    IN      A       89.233.135.60
tm1.cnb.cz.     3600    IN      A       195.144.124.2

;; Query time: 10 msec
;; SERVER: 194.0.12.1
;; WHEN: Mon Feb 26 12:38:34 2024
;; MSG SIZE  rcvd: 152
```

Simulace řešení DNS dotazu
A záznam k www.cnb.cz

```
docm01@4iz110:~$ dig @tm0.cnb.cz. a www.cnb.cz

;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 59318
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.cnb.cz.  IN      A

;; ANSWER SECTION:
www.cnb.cz.     3600    IN      A       193.85.3.250

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 7 msec
;; SERVER: 89.233.135.60
;; WHEN: Mon Feb 26 12:40:25 2024
;; MSG SIZE  rcvd: 44
```

Doménová jména

WHOIS

Michal Ročkai

Doménová jména

- obchodní artikl, dají se koupit, přeprodat, apod.
- TLD jsou velmi nákladné, domény 2. řádu si může dovolit i soukromá osoba
  - některé TLD jsou omezené (pro typ subjektu, účel, apod.)
  - různé ceny dle `TLD`
  - `.cz` doména patří k nejlevnějším
- správce TLD využívá tzv. **registrátory** (`registrar`), se kterými má uzavřené smlouvy a u kterých si registrují domény koncoví uživatelé
- pozor, **`registrar`** (registrátor) zní skoro stejně jako **`registrant`** (majitel domény)!

TLD

- generické (gTLD) se dělí na:
  - běžné (generic) – pro běžné účely (.com, .info, .net, .org)
  - sponzorované (sponsored) – pouze pro entity v daném odvětví (.aero, .asia, .cat, .coop, .edu, .gov, .int, .jobs, .mil, .mobi, .te, .travel, a .xxx)
  - běžné omezené (generic restricted) – pouze pro daný účel (.biz, .name, .pro)
  - infrastrukturní (infrastructure) – prostřednictvím nich se realizuje funkčnost v DNS (.arpa a reverzní záznamy)
  - nové – řada nových TLD, pozor na kolísání cen (.photo, .africa, .cheap, .contractors, .football, .yokohama),
- národní (Country Code TLD) – cz, sk, de, atd., národní domény jsou stanoveny dle standardu ISO 3166-1 alpha-2
- IDN (Internationalized Domain Names) – doménová jména se znaky národních abeced

whois

- veřejné databáze obsahující informace o doménových jménech a IP adresách
  - informace o vlastnících, správcích a další údaje
- WHOIS protokol (RFC 812, r. 1982) je aplikační protokol (**TCP** port **43**) pracující na textové bázi, kterým se získávají data z whois databází
- řádkový nástroj **whois** (**VŠE**: jen **4iz110.vse.cz**)
- do Windows existuje varianta v nástrojích od Sysinternals, ale na VŠE není nainstalovaná
- existují online whois nástroje, obvykle s chybami, jinými problémy a reklamami

Klienti whois

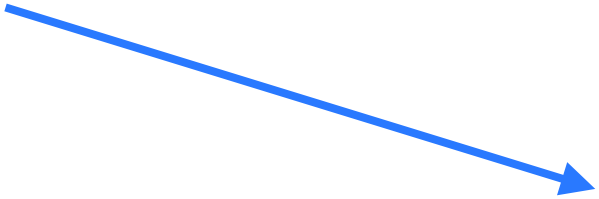
- řádkový klient `WHOIS`:
  - hledání domény: **`whois vse.cz`**
  - hledání IP adresy: **`whois 146.102.18.43`**
- příklad: `whois cnb.cz`

```
domain:         cnb.cz
registrant:     SB:TM358-RIPE_XX
admin-c:        ZIRNSAK
nsset:          CNB
keyset:         AUTO-6L2Z5NYOAB1UFNTURAVDC6IMW
registrar:      REG-WEBGLOBE
registered:     06.03.1997 01:00:00
changed:        04.04.2020 08:27:05
expire:         10.10.2024
...
```

Struktura whois záznamu

Úvodní sekce obsahuje základní informace a odkazy na příslušné **kontakty**, které bývají rozvedeny níže.

```
domain:         cnb.cz
registrant:     SB:TM358-RIPE_XX
admin-c:        ZIRNSAK
nsset:          CNB
registrar:      REG-WEBGLOBE
registered:     06.03.1997 01:00:00
changed:        04.04.2020 08:27:05
expire:         10.10.2024
...
```



níže:

```
contact:        SB:TM358-RIPE_XX
org:            Czech National Bank
name:           Czech National Bank
address:        Na Prikope 28
address:        Praha 1
address:        11503
address:        CZ
registrar:      REG-WEBGLOBE
created:        10.08.2001 22:13:00
changed:        15.05.2018 21:32:00
```

Obsah whois záznamů

- doména má svoje datum zaregistrování i datum expirace (*neprodlouží-li vlastník doménu zaplacením poplatku, doména propadá a může si ji zaregistrovat někdo jiný*)
- povinné jsou kontakty **vlastníka** (`registrant`), což může být `person` nebo `organisation` a kontakt na **registrátora** (`registrar`)
- doména může mít **administrativní** (`admin-c`) nebo **technický** (`tech-c`) kontakt
- doména má ve whois databázi také sadu DNS serverů (`NSSET`) a `DNSSEC` klíče (`KEYSET`)

Bezpečnost DNS

DNSSEC

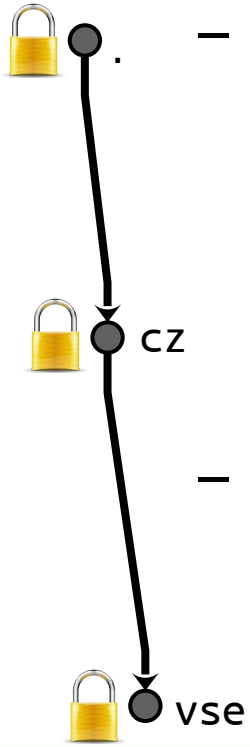
Michal Nečaský

DNS cache poisoning

- způsob, jak zmanipulovat cache rekuzoru, aby vracela útočníkem podvržená data
- princip útoku
  - uživatel/útočník odešle dotaz na rekurzor
  - rekurzor požádá autoritativní server o záznam
  - útočník předstírá identitu autoritativního NS a zašle na rekurzor falešný záznam před tím, než dorazí odpověď ze skutečného autoritativního NS
  - falzifikovaná odpověď útočníka se dostává do cache
- úpravy DNS protokolu zajistily pouze snížení šance na úspěch, ale nezamezily jej

DNSSEC

- **DNSSEC** = DNS Security Extensions
  - **digitální podepisování** a **ověřování** DNS záznamů
  - řeší DNS cache poisoning a další MITM útoky na DNS, ale ne úplně všechny
  - **řetěz důvěry** (*chain of trust*) – podepsaný musí být celý řetěz počínaje záznamy kořenových NS přes záznamy TLD NS až po záznamy NS cílové domény
    - podpisům kořenových NS se věří (nejsou přes DNSSEC ověřitelné) – **kotva důvěry** (trust anchor)
  - podpisy i veřejné klíče jsou **uloženy v DNS** jako speciální **DNS záznamy**



RRset

pro zajímavost

- **R**esource **R**ecord **set** – sada DNS záznamů k podpisu
- podepisují se **všechny** záznamy daného **typu** pro dané doménové **jméno** – tzn. je-li jich víc, podepíšou se všechny jako celek, např.:

```
vse.cz.     7211    IN      NS      mx2.vse.cz.
vse.cz.     7211    IN      NS      ns1.vse.cz.
vse.cz.     7211    IN      NS      ns2.vse.cz.
```

```
vse.cz.     7211    IN      RRSIG   NS 13 2 7211
20240303104343 20240218102305 4859 vse.cz.
O9LT2FL0mQx29Wd+XhRLDFkLIWEmnHH9pIwDVtRsTDAa0sNJx9
nUQPmg S+gAKPiVEP04UlOXgz5N8tlM1gue4g==
```

Klíčové typy DNSSEC záznamů

pro zajímavost

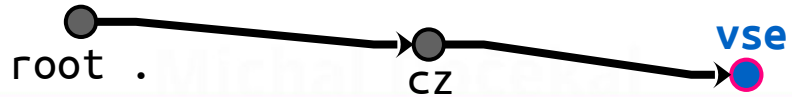
- **RRSIG – digitální podpis** specifický pro **RRset**, který sdružuje záznamy daného typu a doménového jména
  - umístění záznamu: NS server/zóna domény
  - příklad: doménové jméno: **czso.cz**, typ záznamu: **MX**

záznamy (**RRset**):

```
czso.cz.   300   IN   MX       50 smtp3.czso.cz.
czso.cz.   300   IN   MX      300 mspool.gts.cz.
```

podpis (typ **RRSIG**):

```
czso.cz.   300   IN   RRSIG   MX 13 2 300 20240326063637
20240225063637 33072 czso.cz.
UqS/9/7lcINWYzOVx9+crjbm1wjz8kLwvsWd5KxOiy4UI0YZAx4HHn+I
ZCJXzIan35CtMIQ6/q+KPoyDYnTSeA==
```

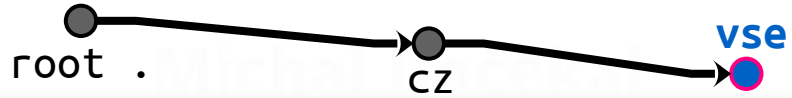


Klíčové typy DNSSEC záznamů

pro zajímavost

- **DNSKEY** – veřejné klíč/klíče, kterými lze ověřit platnost digitálního podpisu RRSIG
  - zone signing key (ZSK, **256**) – klíč podepisující záznamy
  - key signing key (KSK, **257**) – klíč podepisující jen klíče
  - umístění záznamu: NS server/zóna domény

```
czso.cz.  196 IN DNSKEY 256 3 13 /nQy2zr3e4XOvfJLSZG3heo563nN
kPruFFR3vfE1O7VWQafpjOJS+SHSBNOT8ewTOexdxeEUnwoEVvHVle5TaA==
czso.cz. 3196 IN DNSKEY 257 3 13 0EK9ChwJW+CVCvP7mizQwEnR2OJp
HgbLmilGV5OyqncZoOufo9fIbVrv xT6qid/T9sAWH7KOfzItPxkVOIbRjg==
czso.cz. 3196 IN RRSIG DNSKEY 13 2 86400 20240326063637
20240225063637 22941 czso.cz. 2L2nXaPssgyXdA+a6n/YwbUWEfT9U+bMY2cYumm+
vlZ7iUyCmLWxxV45Zp54KkNzMq2wubrA/IULpOjhPRhy6Q==
czso.cz. 3196 IN RRSIG DNSKEY 13 2 86400 20240326063637
20240225063637 33072 czso.cz. 0hJmxg6zudGfFbilSXmstmhwV3ldGw5PjdesQhHs
IuqAJyPB10Xm3Th82lVPhYNmQ6zIKChtiieXa1dC0l+oHA==
```



Klíčové typy DNSSEC záznamů

pro zajímavost

- **DS** – hash DNSKEY záznamu (KSK), kterým lze ověřit platnost DNSKEY
  - používá-li se v zóně jen jeden klíč místo dvou, pak je to ZSK, a v tom případě by DS záznam obsahoval ZSK
  - umístění záznamu: **nadřízený** NS server/zóna

```
vse.cz.  3600  IN  DS 4859 13 2
607BEA3CF352BA4B5EA52BF08B88230097ED3D204B9432400A
314947 CD6E02B8

vse.cz.  3600  IN  RRSIG DS 13 2 3600
20240303174901 20240218161901 47281 cz.
qpa4S0DK0SyCoG8chrFT3hU8NgW1z7xDksIXtXjudbvdtAfPVg
cktVdU 3LuGanHsl/FMCcvBpqnNTigysmwkFg==
```

Proces ověření DNSSEC

pro zajímavost

- rekurzor požádá o RRset, ve kterém se nachází hledaný záznam
  - autoritativní NS vrátí celý RRset a odpovídající záznam RRSIG
- rekurzor požádá o klíče v záznamech DNSKEY
  - autoritativní NS vrátí veřejný ZSK i KSK, které vrátí RRSIG pro RRset záznamů DNSKEY
- ověříme RRSIG požadované sady záznamů (RRset) veřejným ZSK
- ověříme RRSIG sady DNSKEY veřejným KSK

- ověříme platnost KSK dotazem na DS záznam nadřazené zóny
- ověříme nadřazené zóny až ke kořenu DNS

Slabiny DNSSEC

- stále je možné páchat MITM útok, je-li útočník mezi vámi a vaším DNSSEC rekurzorem
- skrytí subdomény je obtížnější
  - mechanismus podepisování negativních odpovědí (záznamy NSEC a NSEC3) bylo/je možné zneužít k objevení „tajných" subdomén (i když skrývání subdomén je security by obscurity)

DANE (DNS-Based Authentication of Named Entities)

pro zajímavost

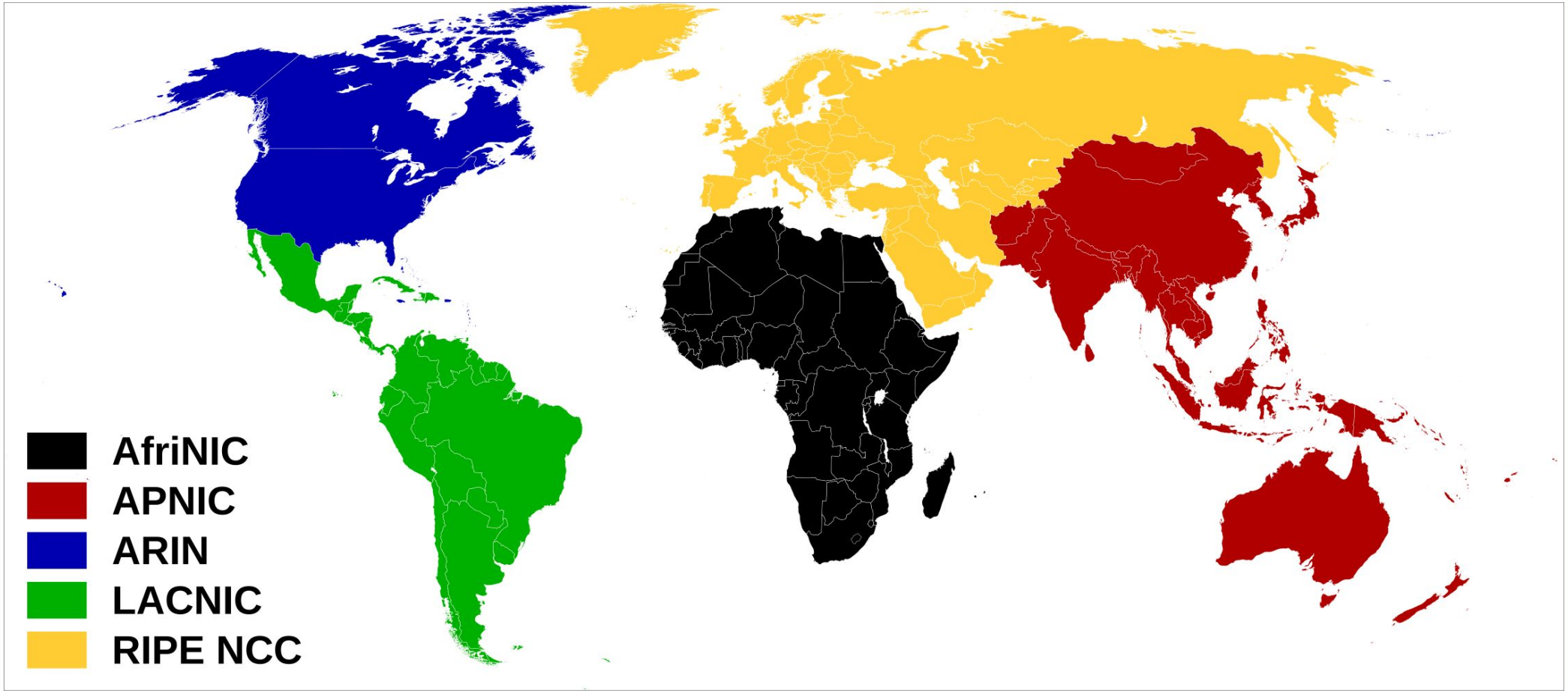
- na DNSSEC staví protokol DANE, který využívá TLSA záznamu ověřeného pomocí DNSSEC k validaci TLS certifikátů pro danou doménu
- alternativa k systému certifikačních autorit pro doménovou validaci
- třeba podpora prohlížečů, která však zatím stále chybí – není vůle (rozšíření mohou řešit)
- TLSA záznam (fingerprint použitého certifikátu):

```
_443._tcp.prales.eu. IN TLSA 3 1 1 123456789ABCDEF
```

Správa/přiřazování IP adres

- **IANA** (**I**nternet **A**ssigned **N**umbers **A**uthority)
  - spravuje kořenové DNS servery, alokuje IP adresy, alokuje čísla AS (autonomních systémů) a další čísla vztažená k fungování počítačových sítí
  - alokace IP adres: IANA přiřazuje IP rozsahy RIRům
  - **RIR** (**R**egional **I**nternet **R**egistry)
    - získává IP rozsahy od IANA
    - přiřazuje IP rozsahy ISPčkům či velkým zákazníkům
      - kteří je přeprodávají nebo spíše pronajímají svým (zpravidla menším) zákazníkům

Struktura RIRů



whois

- kromě informací o doménových jménech obsahují whois databáze i informace o **IP adresách**

```
inetnum:        146.102.0.0 - 146.102.255.255
netname:        VSE-TCZ
descr:          Vysoka skola ekonomicka v Praze
descr:          Prague
country:        CZ
org:            ORG-UoEP1-RIPE
admin-c:        VNO3-RIPE
tech-c:         VNO3-RIPE
status:         LEGACY
mnt-by:         TENCZ-MNT
mnt-routes:     TENCZ-MNT
mnt-by:         RIPE-NCC-LEGACY-MNT
remarks:        Please report network abuse -> abuse@vse.cz
created:        2006-05-18T10:44:11Z
last-modified:  2016-04-14T09:59:42Z
source:         RIPE
sponsoring-org: ORG-CA9-RIPE
```

DNS a jiné aplikační protokoly

- nemálo aplikačních protokolů prorostlo s DNS systémem a závisí na něm nejenom kvůli překladu jména na adresu
- poštovní servery, protokol SMTP
  - MX, SPF, DKIM, DMARC záznamy
- webové servery, protokol HTTP
  - webhosting, virtuální weby (virtual hosts)
- služby využívající SRV záznamy
- atd.

Name based virtual hosts

```
fph.vse.cz.          7200   IN   A    146.102.17.31
fm.vse.cz.           7211   IN   A    146.102.17.31
webhosting.vse.cz.   7195   IN   A    146.102.17.31
```

- více domén směřuje na 1 IP adresu
- jeden server hostuje webové prezentace pro všechny domény
- doménové jméno požadované prezentace je součástí **HTTP** požadavku (hlavička **Host:**)
- podle toho server vrátí požadovanou prezentaci (IP adresa sama o sobě v tomto případě nestačí)

whois

pro zajímavost

- kromě informací o doménových jménech obsahují whois databáze i informace o IP adresách a ***autonomních systémech***

```
% Information related to '146.102.0.0/16AS2852'

route:          146.102.0.0/16
descr:          VSE-TCZ
origin:         AS2852
mnt-by:         AS2852-MNT
remarks:        Please report abuse -> abuse@vse.cz and abuse@cesnet.cz
created:        1970-01-01T00:00:00Z
last-modified:  2006-06-26T13:44:23Z
source:         RIPE
```

- https://www.peeringdb.com/

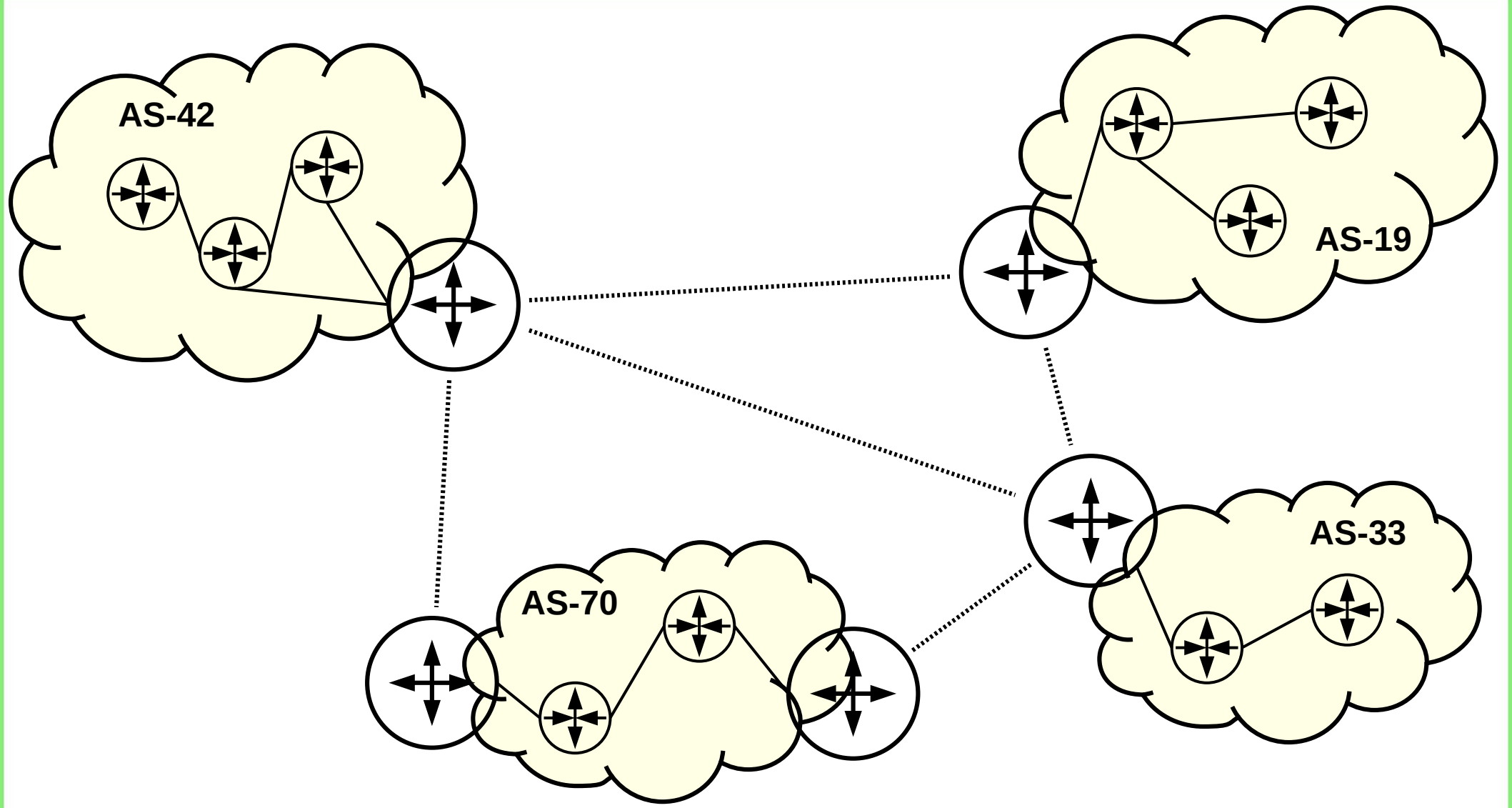
Autonomní systémy

pro zajímavost

- **internet** je rozdělen na jednotky, které se nazývají *autonomní systémy*
- **autonomní systém (AS)** je část internetu pod správou konkrétního subjektu s jednotnou směrovací politikou (z hlediska internetu)
- **AS** si řeší směrování uvnitř **AS** sám
- směrování síťového provozu mezi **AS** řeší hraniční routery

Autonomní systémy

pro zajímavost



Děkuji za pozornost

Michal Pačelka