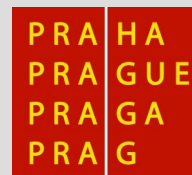


# Y36SPS

## Jmenné služby DHCP a DNS

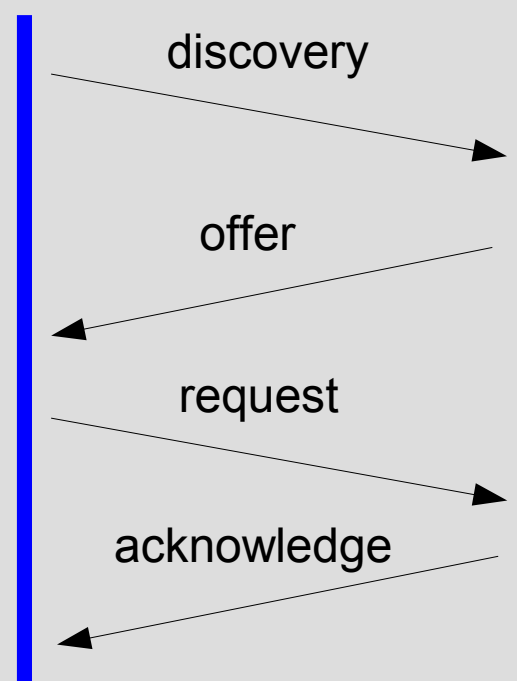


# Dynamic host configuration protocol (DHCP)

- 1993
- RFC2131
- přidělení parametrů při startu
  - IP adresa, maska, směrovače ...
- přidělení IP adresy
  - dynamické
  - automatické
  - manuální
- chybí autentizace (RFC3118)
- alternativy
  - BootP, RARP, IPv6 (DHCPv6, bezstavové)

# DHCP komunikace

- server 67/udp
- klient 68/udp
  
- discovery
- offer
- request
- acknowledge
- information
- releasing



# DHCP - parametry

- vendor
  - subnet mask, time offset, routery, time servery, name servery, log servery, lpr servery
- IP
  - forwarding, MTU, broadcast, static route, TTL
- link
  - ARP cache timeout, ethernet II / IEEE802.3
- TCP
  - TCP default TTL, TCP keepalive
- aplikace
  - NIS servery, SMTP servery, POP3 servery
- DHCP
  - adresa, lease time, bootování

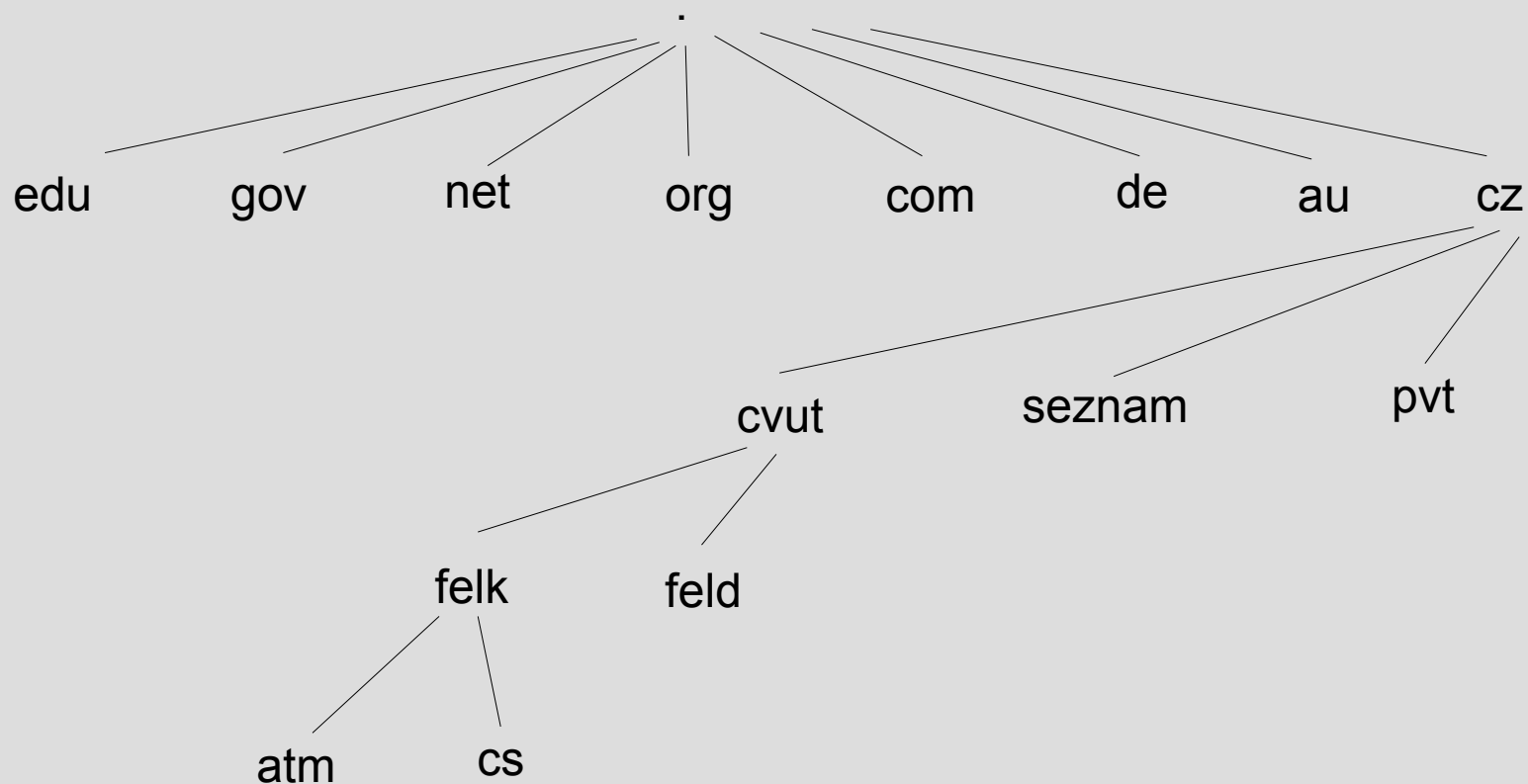
# DNS

- Domain Name System – rfc1034, rfc1035 ...
- primárně určen pro překlad jméno – adresa
- vychází z host.txt
- informace
  - A 32b IP adresa
  - NS autoritativní jmenný server
  - CNAME synonymum ke jménu
  - SOA start of authority
  - PTR reverzní překlad
  - HINFO popis SW a HW
  - MX preference a jméno mail serveru
  - TXT textový řetězec
  - AAAA 128b IP adresa
  - ...

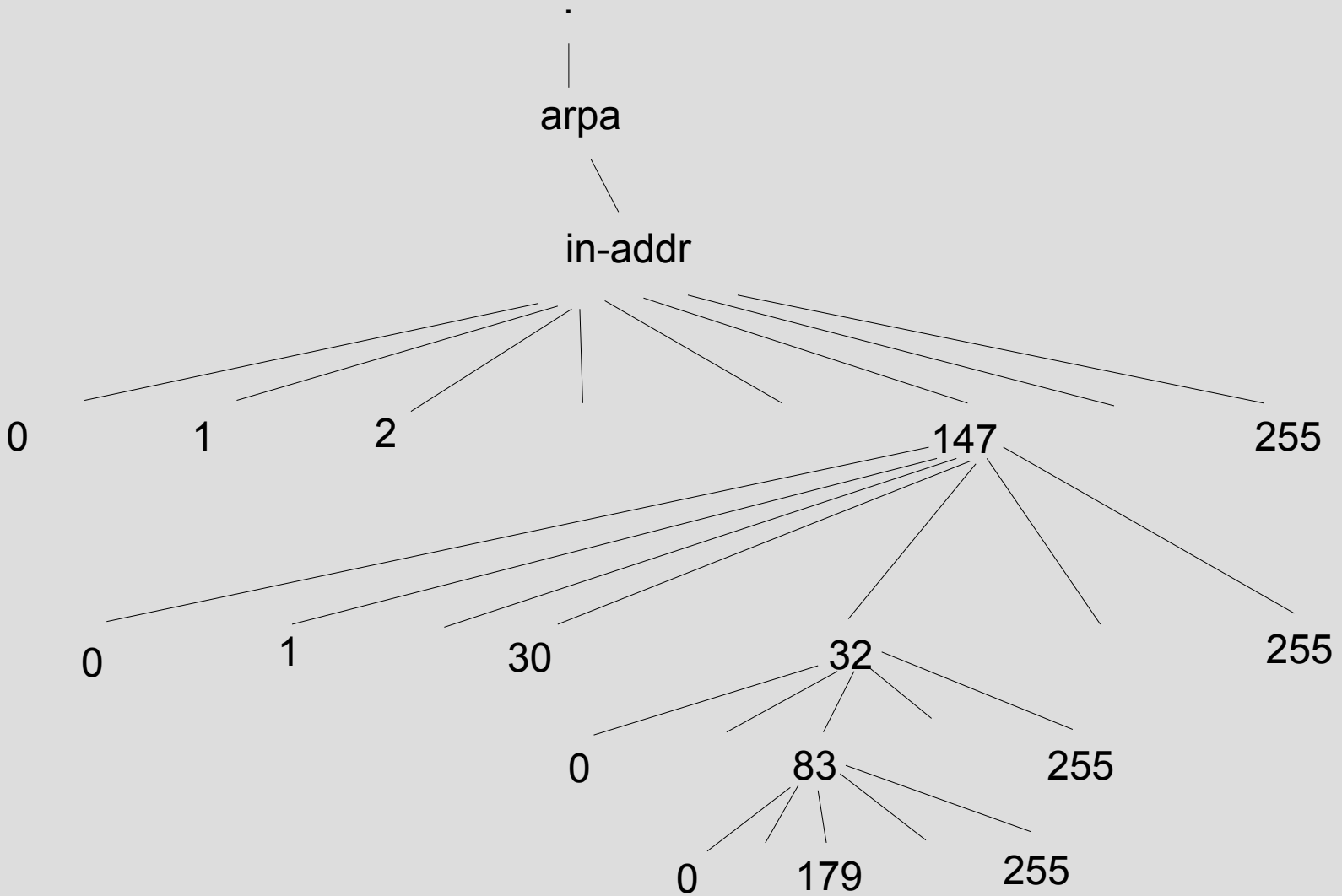
# DNS komponenty

- jmenný prostor a zdrojové záznamy
  - stromová struktura
  - jméno 0 – 63 B, celkově max. 255 B
  - absolutní jméno - atm.felk.cvut.cz.
  - relativní jméno - atm
- jmenné servery
  - datové sklady vytvářející jmennou databázi
  - odpovídají na dotazy
  - synchronizují databázi
  - udržují mezipaměť odpovědí
- resolvers
  - soustava knihovných funkcí zaručující překlad
  - je součástí klienta i DNS serveru

# DNS domény



# DNS reverzní doména





# DNS - typy serverů

- primární
  - udržuje data o zóně
  - autoritativní server
- sekundární
  - kopíruje si data z primárního serveru
  - autoritativní server
- caching only
  - není autoritativní pro žádnou zónu (na rozdíl od pri. a sek.)
- root
  - udržuje záznamy root domény
- forwarding
  - předává rekurzivní dotaz (odlehčení linky), může sám resolvovat
- slave
  - jen forwarding (problém s terminologií)

# DNS komunikace

- protokol TCP i UDP
- port 53/udp, 53/tcp
- UDP max 512B – jinak TCP
- zone transfer – TCP
- dotaz se posílá na víc serverů
  - první odpověď je platná, ostatní se zahodí
  - možnost nekonzistence nameserverů
- dns dotaz, dns odpověď
  - rekurzivní dotaz a odpověď
- dns update
  - podpora pro ddns; informace o zóně, předpoklady, update

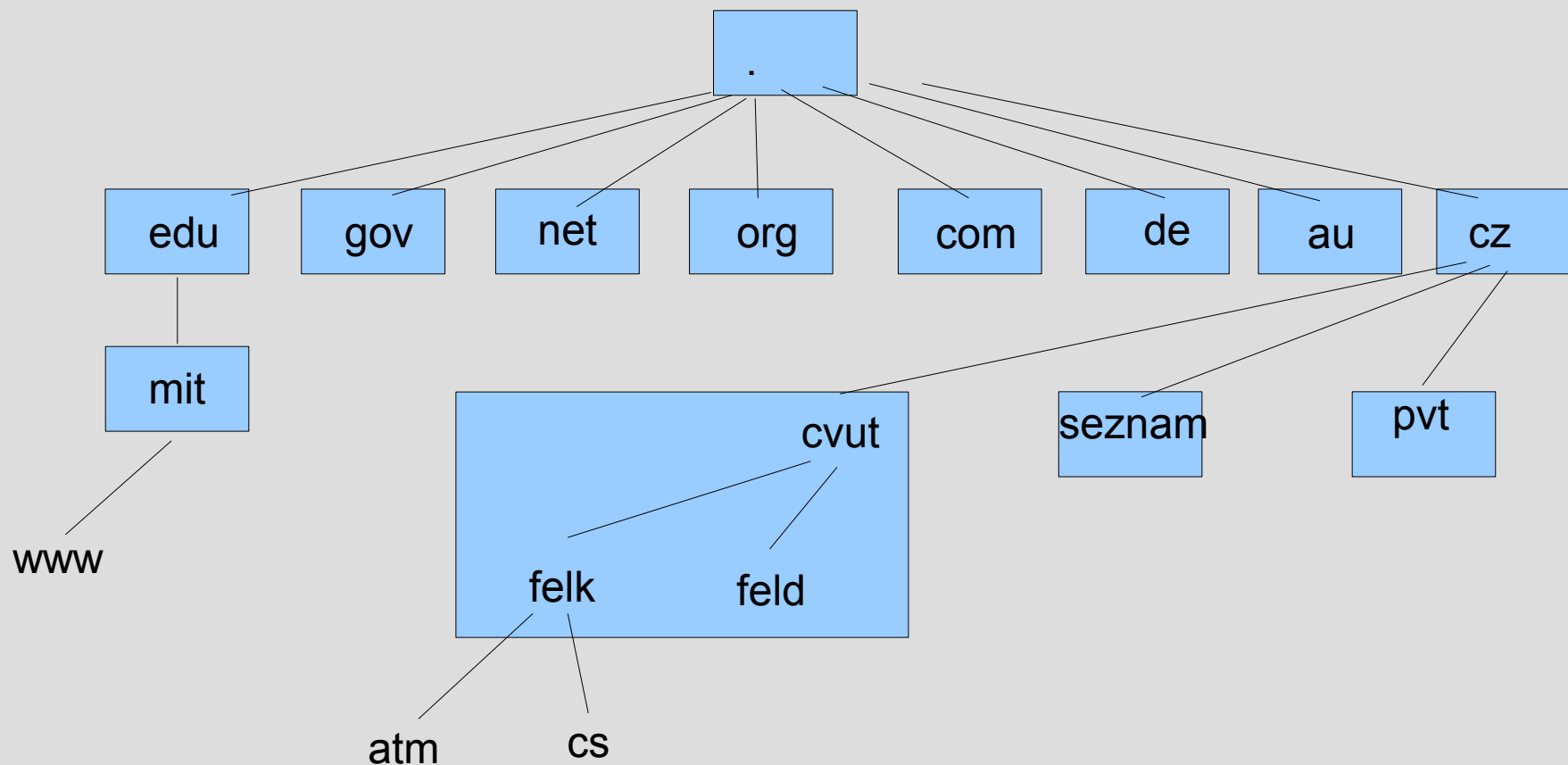
# DNS komunikace II

- pozitivní, negativní caching
- dns notify
  - informace sekundárním serverům o změně
- replikace primárního serveru
  - inkrementální zone transfer
- autentizace

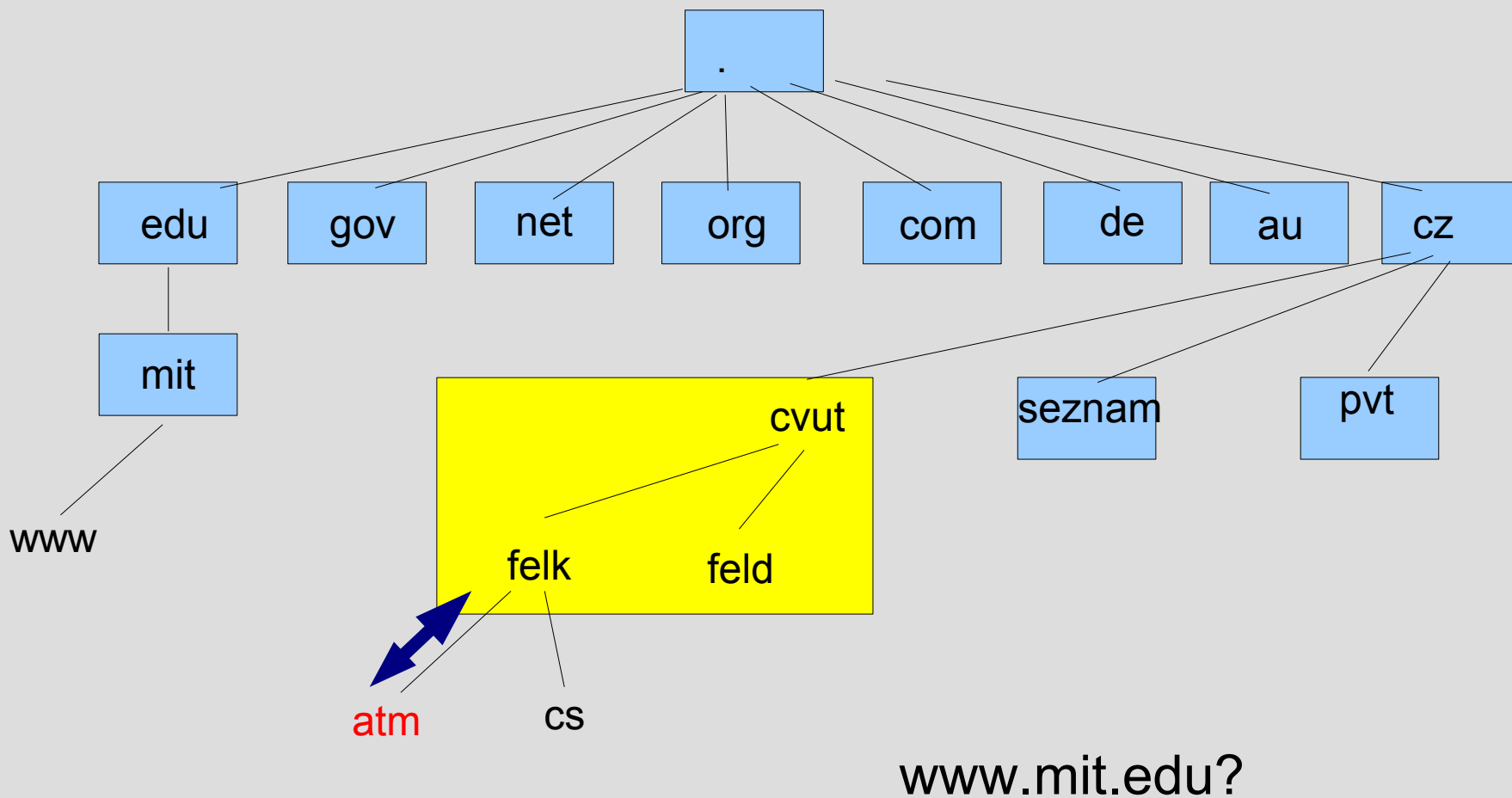
# DNS dotaz

- může být zodpovězen autoritativně i neautoritativně
- pokud server nezná odpověď – obrací se na **root** **servery** a potom postupuje směrem k subdoménám podle NS záznamů
- může být vyžadován UDP checksum
- omezení UDP odpovědi na 512B
- obsahem odpovědi je i doba platnosti

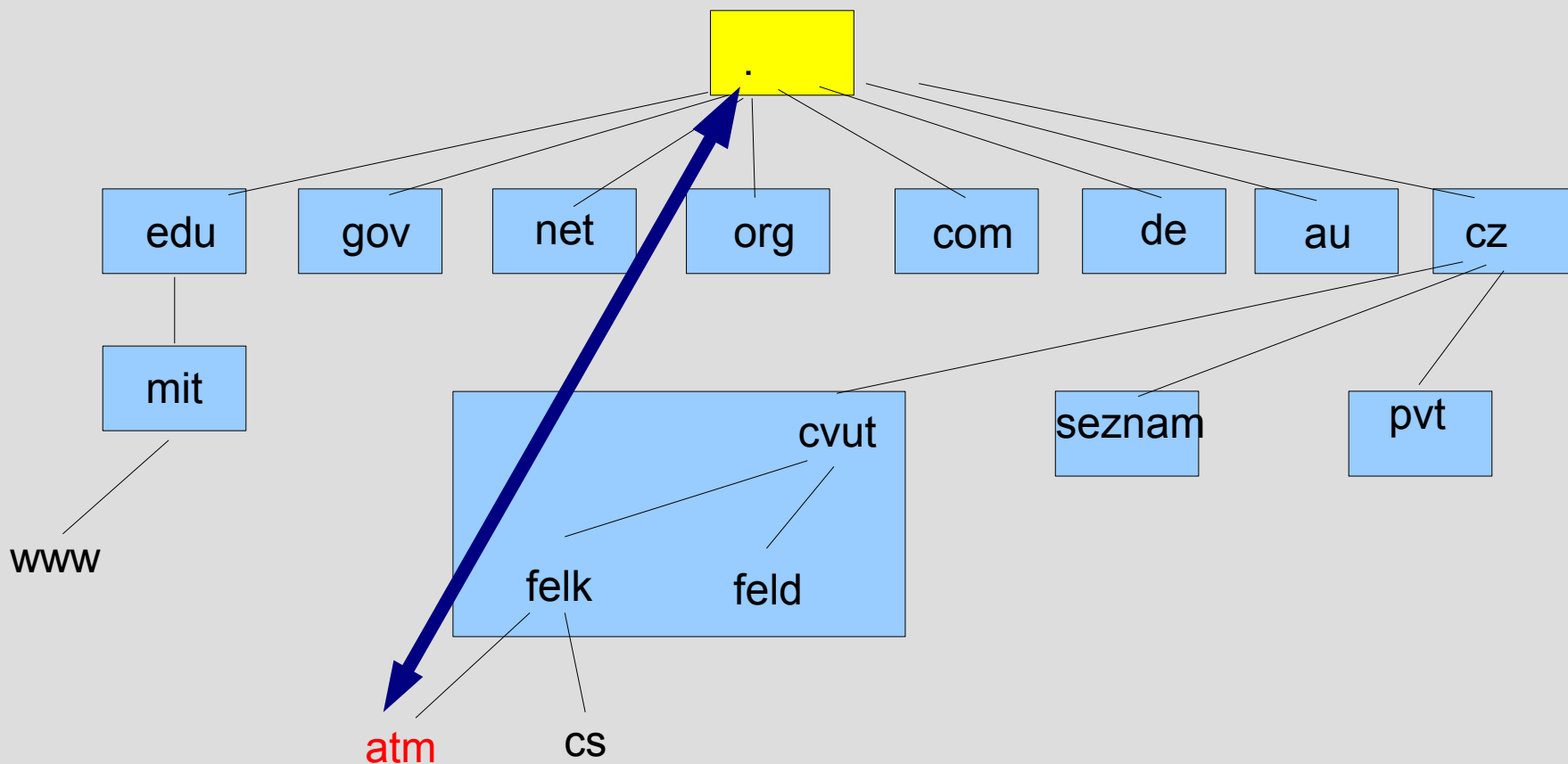
# DNS dotaz



# DNS dotaz - nerekurzivní

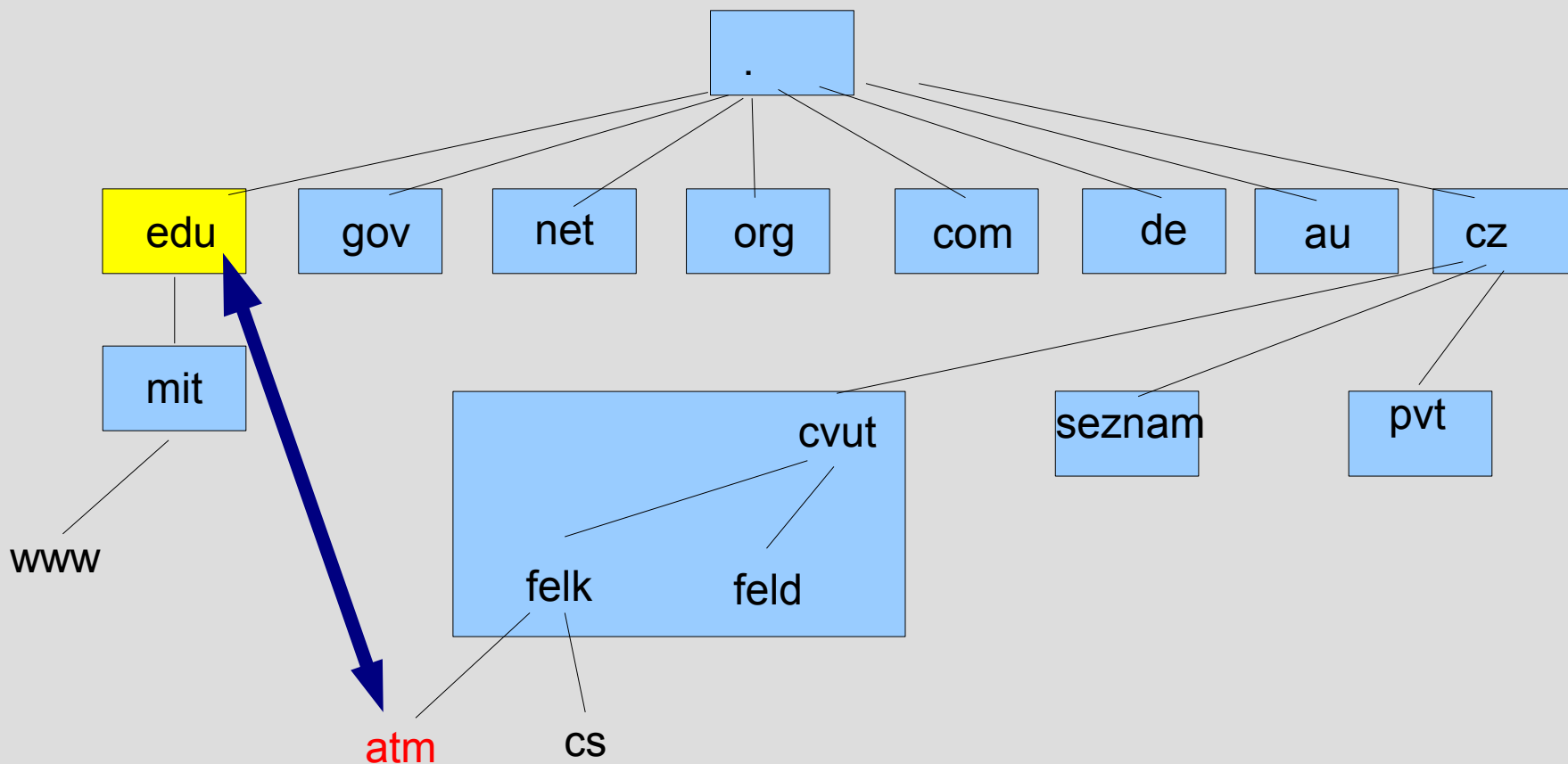


# DNS dotaz - nerekurzivní



www.mit.edu?

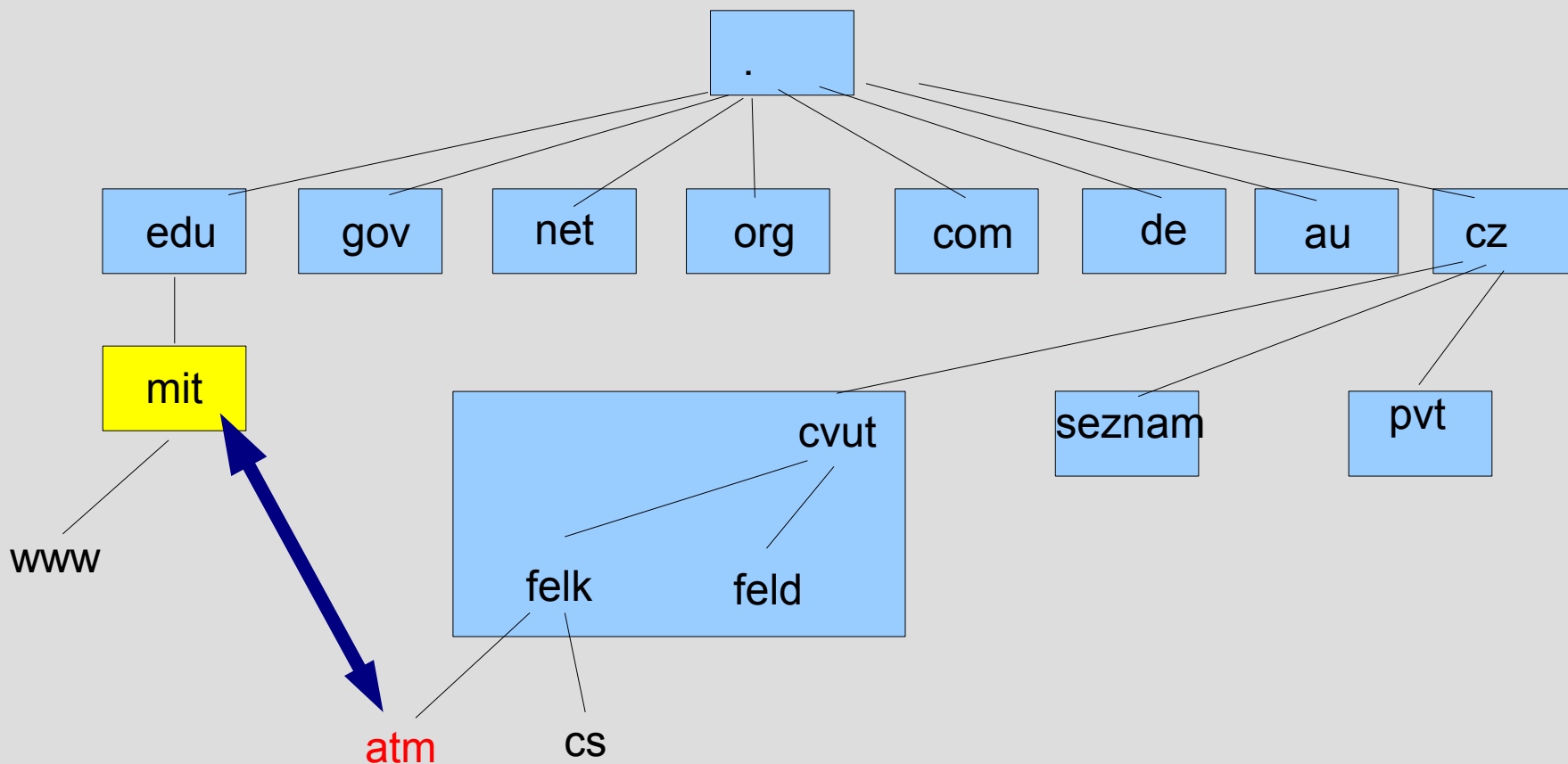
# DNS dotaz - nerekurzivní



`www.mit.edu?`

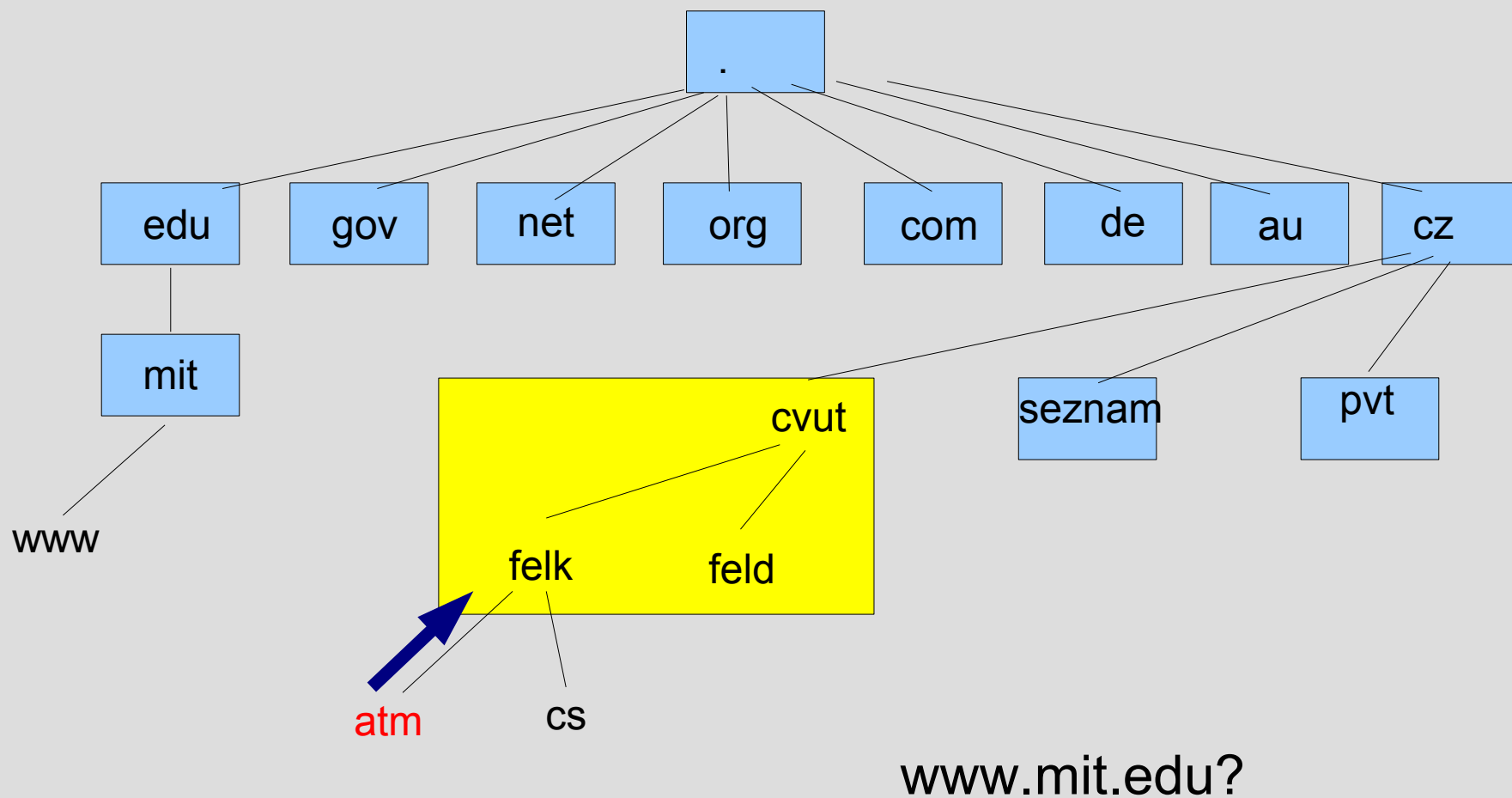


# DNS dotaz - nerekurzivní

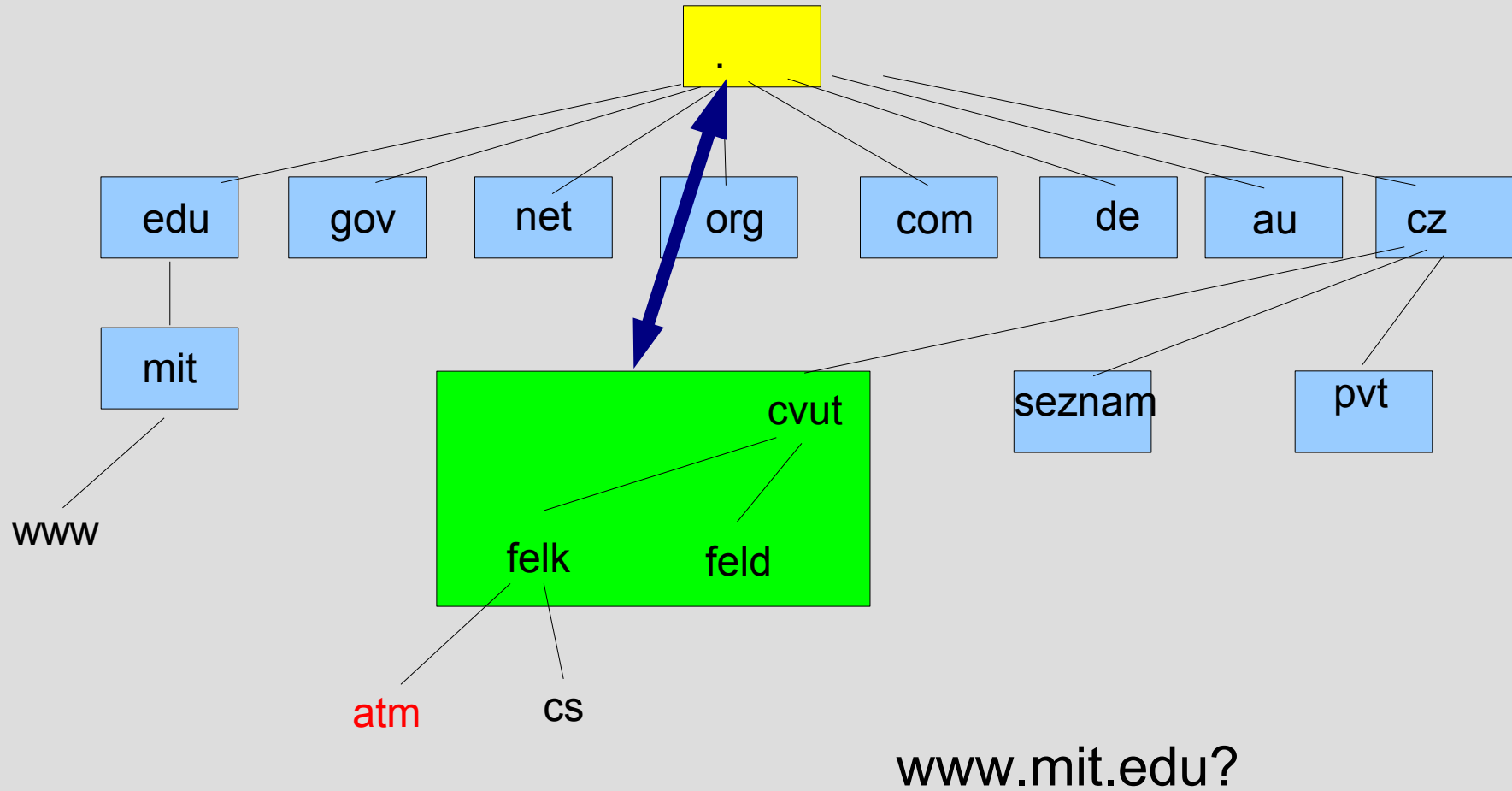


www.mit.edu=18.7.22.83

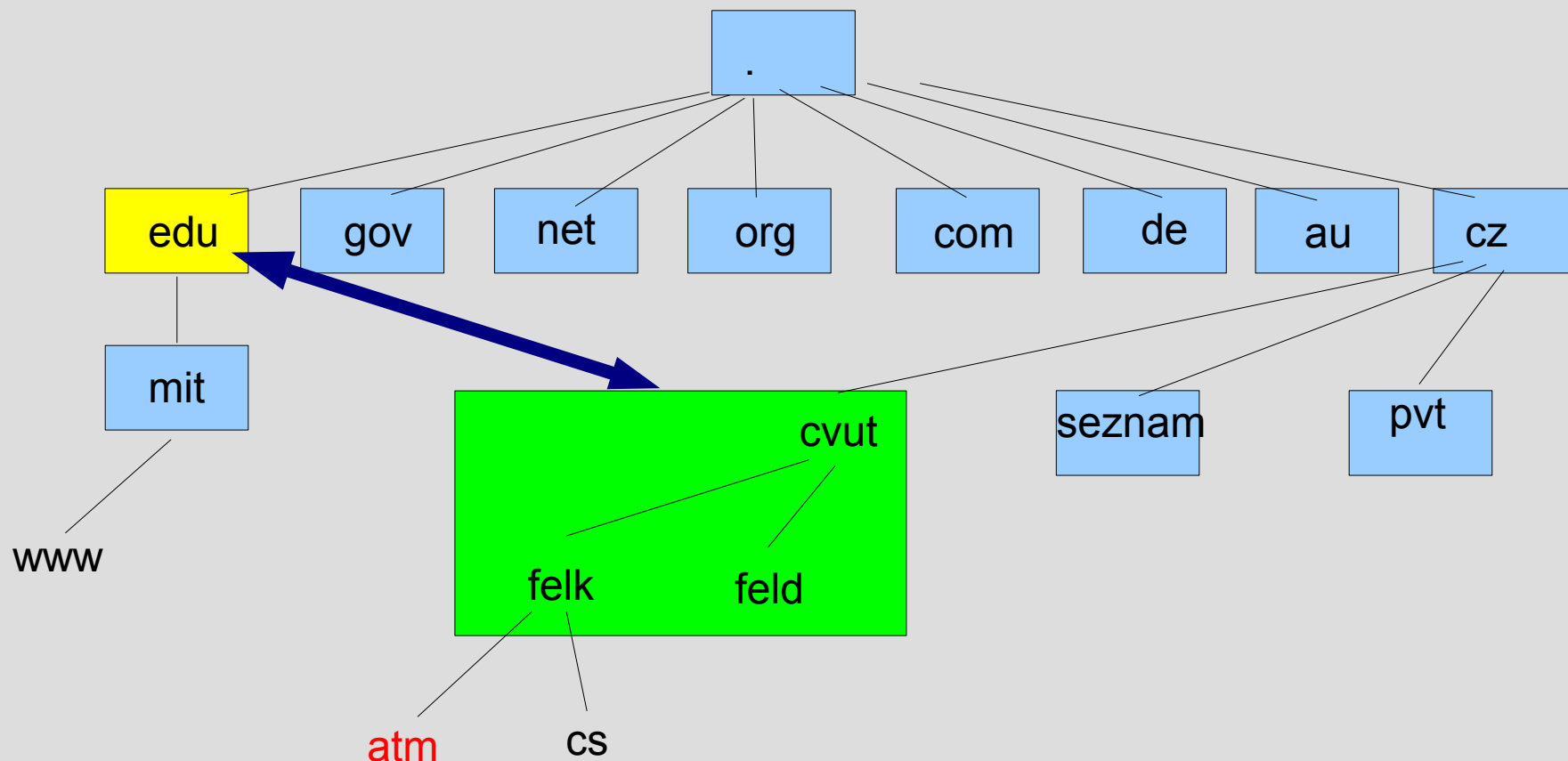
# DNS dotaz - rekurzivní



# DNS dotaz - rekurzivní

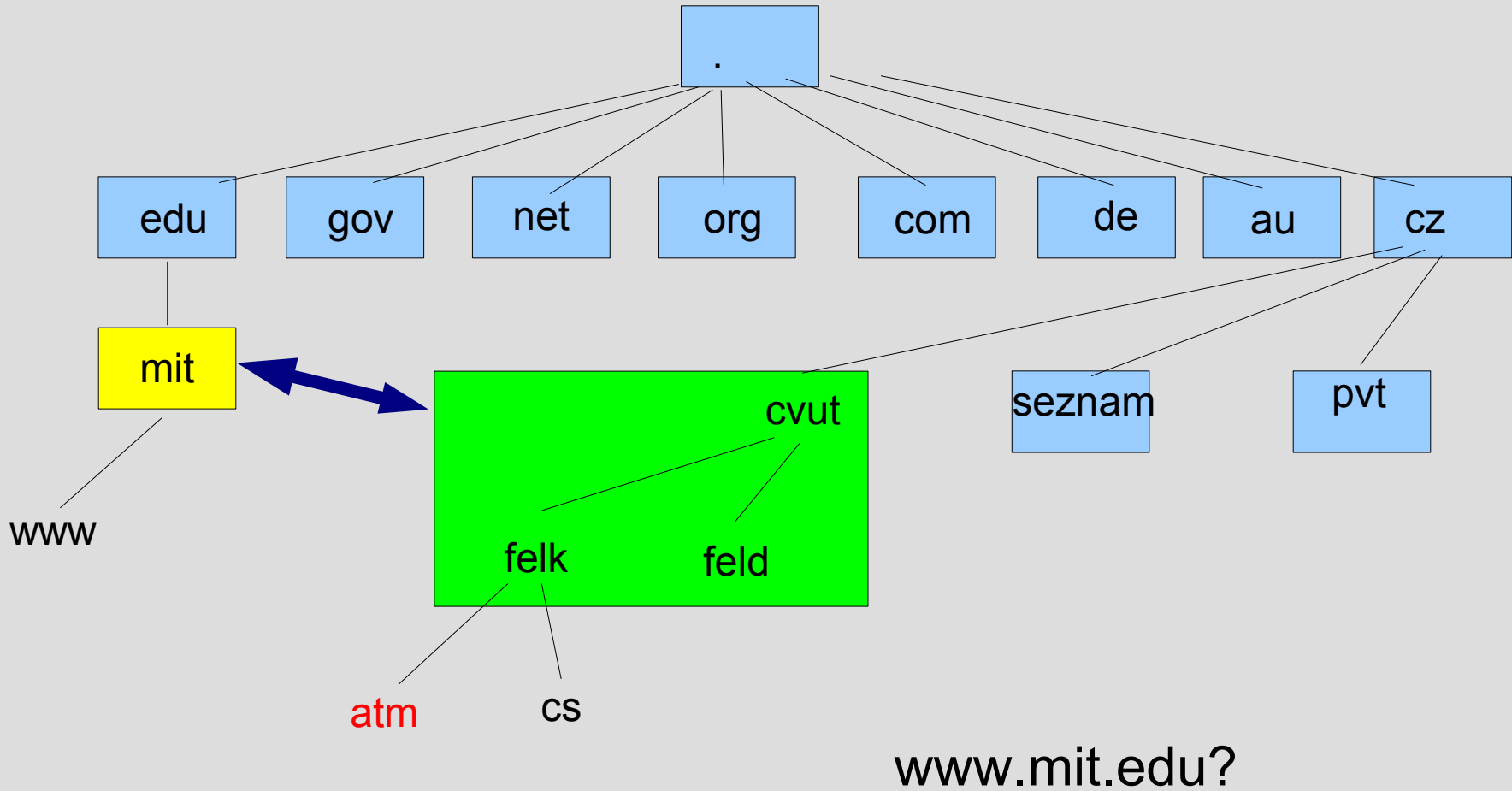


# DNS dotaz - rekurzivní

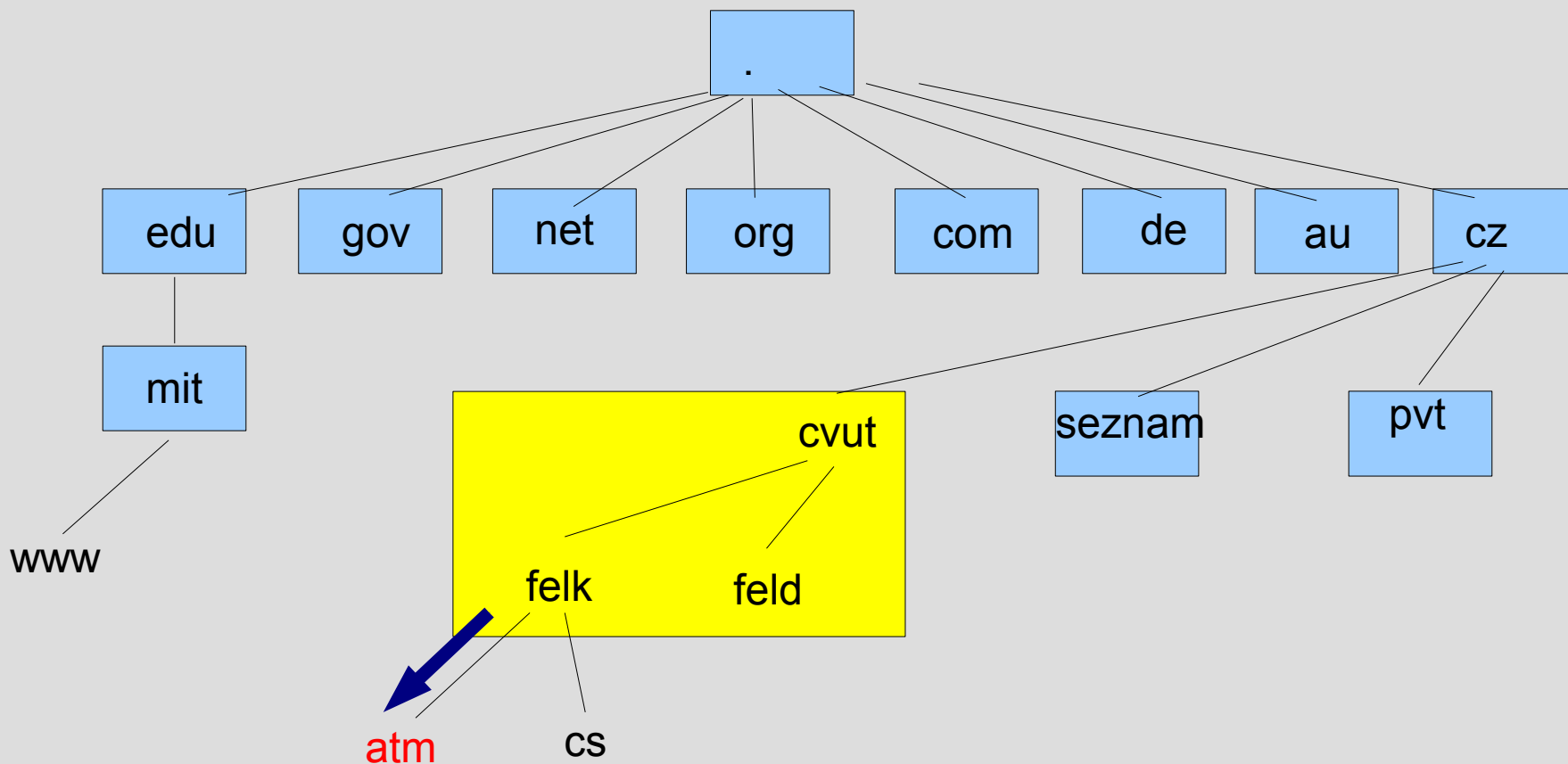


`www.mit.edu?`

# DNS dotaz - rekurzivní



# DNS dotaz - rekurzivní



www.mit.edu=18.7.22.83

# DNS update

- rfc2136, podpora pro ddns
- odebrání/přidání vět do zónového souboru
- nelze přidat další zónu
- operace
  - zóna
  - předpoklad
    - existence/neexistence vět v zóně na primárním serveru
  - update
    - přidat věty
    - zrušit sadu vět daného typu
    - zrušit všechny věty daného jména
    - zrušit jednu větu
- zabezpečení
  - secure dynamic update (rfc2137)
  - update jen z vybraných adres

# SOA záznam

- start of authority
- uvozuje soubor zóny

```
@ IN SOA ns.fel.cz. master.fel.cz {  
2008032501 ;serial  
86400 ;refresh 24h (sek.)  
600 ;retry 10m (sek.)  
120960 ;expire 2w (sek.)  
86400} ;minimum TTL (odp.)
```

- @ ... fel.cz.



# A záznam

- přiřazení jméno – adresa

fel.cz.            IN    SOA ...

www            IN    A    194.22.23.129

www.fel.cz.    IN    A    194.22.23.130

ns            IN    A    15.2.2.2

# CNAME záznam

- synonyma (aliasy) ke jménům
- na pravé straně nesmí být alias
- je lepší psát úplné jméno

fel.cz.	IN	SOA ...	
itchy	IN	A	194.22.23.130
www	IN	CNAME	itchy.fel.cz.
<del>ftp</del>	<del>IN</del>	<del>CNAME</del>	<del>www.fel.cz.</del>

# NS záznam

- definice autoritativních serverů
- uvedeny v nadřízené doméně
- uvedeny na autoritativním serveru ve vlastní doméně
- pravá strana nesmí být CNAME

cz.	IN	SOA ...	
	IN	NS	ns.cz.
ns	IN	A	194.11.11.11
fel	IN	NS	ns.cz.
	IN	NS	ns.fel.cz.
ns.fel	IN	A	194.22.23.130
fel.cz.	IN	SOA ...	
	IN	NS	ns.cz.
	IN	NS	ns.fel.cz.
ns	IN	A	194.22.23.130

# MX záznam

- poštovní server pro doménu
- umožňuje určit prioritu (nižší číslo je lepší)

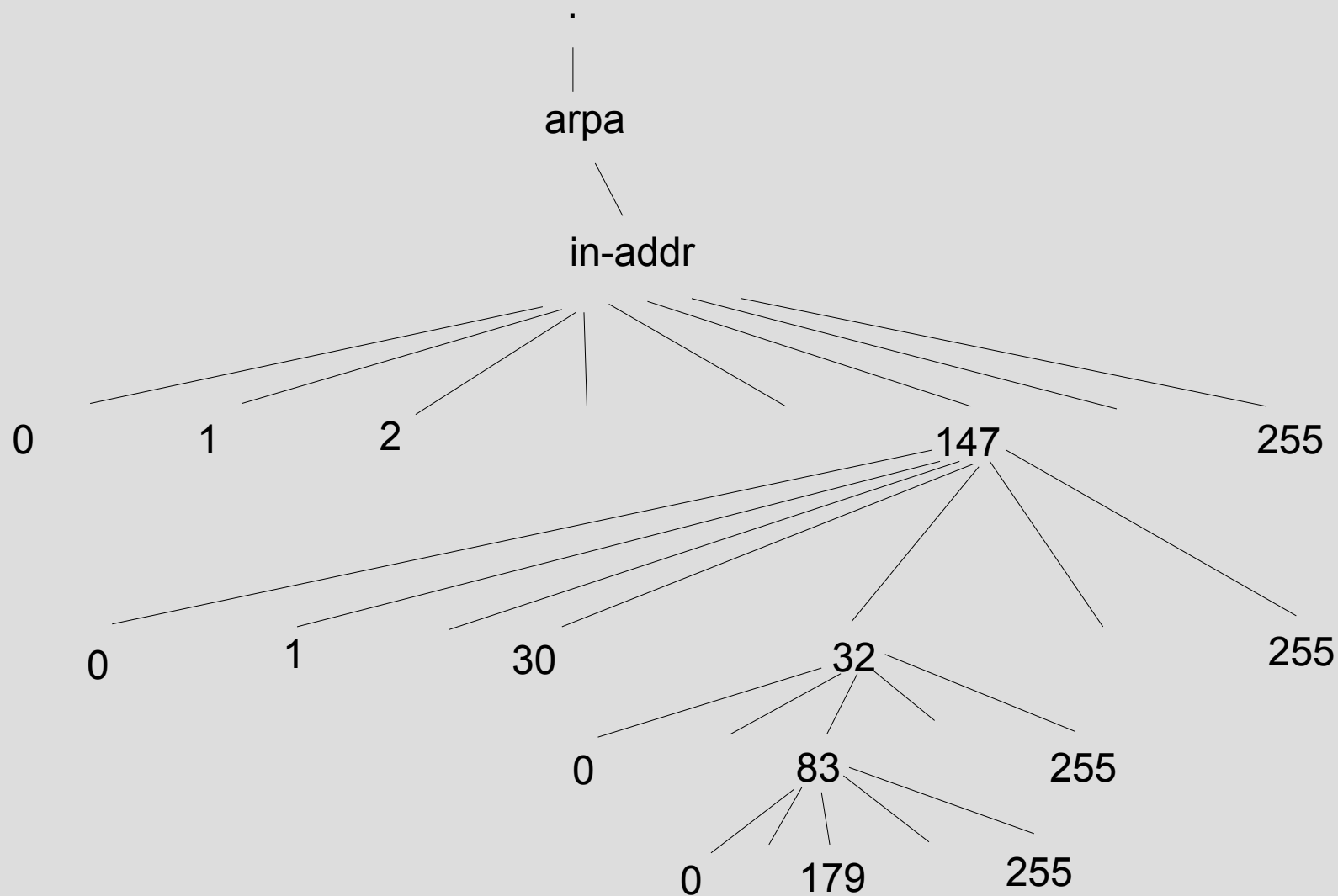
fel.cz.	IN	SOA ...		
	IN	MX	10	mail.fel.cz.
	IN	MX	20	mail1.fel.cz.
mail	IN	A	194.22.23.131	
mail1	IN	A	15.2.2.3	

# PTR záznam

- překlad IP adresa – jméno
- doména in-addr.arpa.

```
23.22.194.in-addr.arpa. IN SOA ...  
130 IN PTR www.fel.cz.  
131 IN PTR mail.fel.cz.
```

# Reverzní dotaz



# Reverzní dotaz – delegace

- ns.ripe.net

```
194.in-addr.arpa. IN SOA ...  
23.22 IN NS ns.fel.cz.
```

- ns.fel.cz

```
23.22.194.in-addr.arpa. IN SOA ...  
IN NS ns.fel.cz.  
130 IN PTR www.fel.cz.  
131 IN PTR mail.fel.cz.
```

# Reverzní dotaz – subnet

- 194.22.23.0/24
- 23.22.194.in-addr.arpa
  - 129.23.22.194.in-addr.arpa
- 194.22.23.128/25
- 128.23.22.194.in-addr.arpa
  - 129.128.23.22.in-addr.arpa



# Subnet – delegace

```
23.22.194.in-addr.arpa. IN SOA ...  
      IN NS ns.fel.cz.  
126   IN PTR ns.fel.cz.  
128   IN NS ns.kp.fel.cz.  
130   IN CNAME 130.128.23.22.194.in-addr.arpa.  
131   IN CNAME 131.128.23.22.194.in-addr.arpa.
```

```
128.23.22.194.in-addr.arpa. IN SOA ...  
      IN NS ns.kp.fel.cz.  
130   IN PTR www.fel.cz.  
131   IN PTR mail.kp.fel.cz.
```

# Speciality

- DNS na uzavřené síti
  - odpovědi na chybné dotazy
  - vybudování root serveru
- DNS za firewallem
- DNS pro intranet a internet
  - doména local
  - duální DNS

- DHCP
  - rfc2131
    - rfc3315
- DNS
  - Dostálek L., Kabelová A.; Velký průvodce protokoly TCP/IP a systémem DNS; ...
  - rfc1034, rfc1035
  - rfc2136
  - ...