



dsn

# X36PKO

## Jmenné služby

# Program

- úloha jmenných služeb
- informace ve jmenných službách
- jmenné služby
  - X.500
  - DNS
  - ostatní

# Úloha jmenných služeb

- specializovaná databáze
  - adresář,
  - optimalizace pro čtení a vyhledávání,
  - občasné aktualizace,
  - distribuce,
  - replikace,
  - chybí podpora transakcí.
- úlohy
  - překlad,
  - ověření,
  - vyhledání (lokalizace),
  - poskytování podrobných informací (vlastností).

# Jmenné služby

- soubory
- X.500
- LDAP - Lightweight Directory Access Protocol
- DNS - Domain Name System
- NIS – Network Information Service
- CDS - Cell Directory Service
- MS Active Directory
- ...

# X.500

- CCITT X.500 - X.521
- 1988 – ISO 9594
- hierarchický jmenný prostor
- komunikace klient – server
  - DAP (Directory Access Protocol)
    - OSI protokol
  - LDAP (Lightweight Directory Access Protocol)
    - TCP/IP, vynechané funkce, nedefinuje adresář
    - původně jen přístupový protokol k X.500 serveru
    - postupně vznikl LDAP server
- decentralizovaný, jednotný globální prostor, podpora libovolných atributů, složité dotazy, podpora autentizace, ACL

# X.500 - organizace dat

- záznam – relativní jedinečné jméno (Relative Distinguished Name)
  - jeden nebo více atributů
- jedinečné jméno (Distinguished Name) – posloupnost všech relativních jedinečných jmen od kořene
- atributy (X.520)
  - C Country, SP State or Province, L Locality, O Organization, OU Organization Unit, CN Common Name
- příklady
  - CN=Jan Kubr, C=CZ
  - CN=Jan Kubr, O=CVUT, C=CZ
  - CN=CVUT, C=CZ
  - CN=atm.felk.cvut.cz, OU=FELK, O=CVUT, C=CZ

# LDAP datový model

- záznam
  - identifikován DN.
- atributy
  - tvoří záznam,
  - jméno,
  - typ,
  - hodnoty.
- typy
  - int,
  - bin,
  - cis,
  - ces,
  - dn,
  - tel.
- třídy – objectclass
  - definice atributů,
  - standardní třídy,
  - uživatelské třídy.
- DIT - Directory Information Tree
  - struktura adresářového stromu.
- odkaz na jiný LDAP server
  - atribut ref a LDAP URL
  - <ldap://ldap.cvut.cz/o=cvut,c=cz>

# LDAP funkce

- LDAP - rfc2251-6
- dotazování a prohledávání
  - search,
  - compare.
- změny dat
  - add,
  - delete,
  - modify,
  - modifyRDN.
- autentizace
  - abandon,
  - bind,
  - unbind.
- možnost definovat vlastní operace.



# Aplikace využívající LDAP

- servery
  - University of Michigan LDAP server,
  - OpenLDAP server,
  - iPlanet Directory Server,
  - Active Directory.
- email klienti
  - MS Outlook, MS Outlook Express - Adresář,
  - Evolution,
  - Thunderbird.
- samostatní klienti
  - LDAPconf,
  - OpenLDAP.
- Samba
- LDAP PAM
- ...

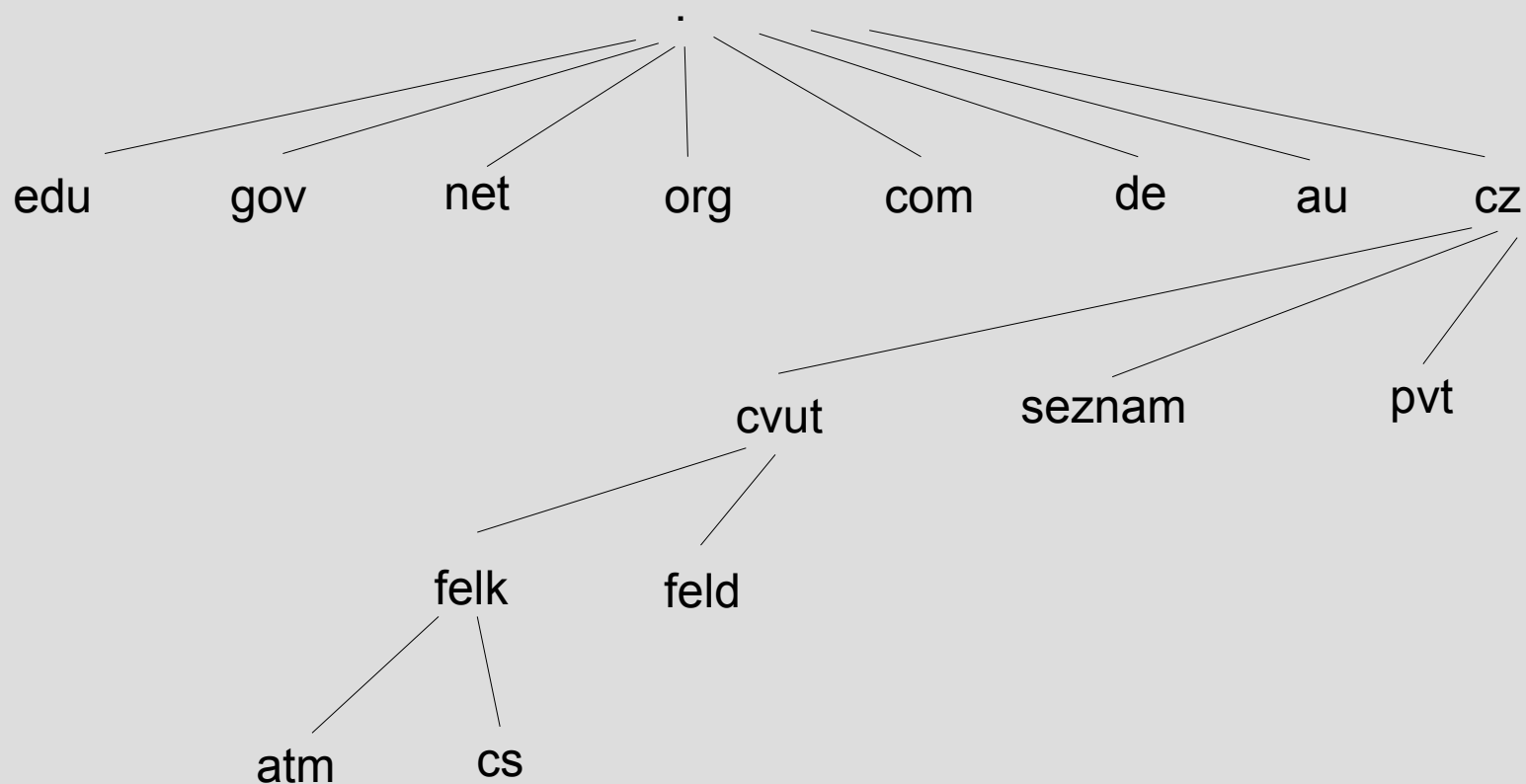
# DNS

- Domain Name System – rfc1024, rfc1025 ...
- 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
- resolvery
  - soustava knihovnických funkcí zaručující překlad
  - je součástí klienta i DNS serveru

# DNS domény



# 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

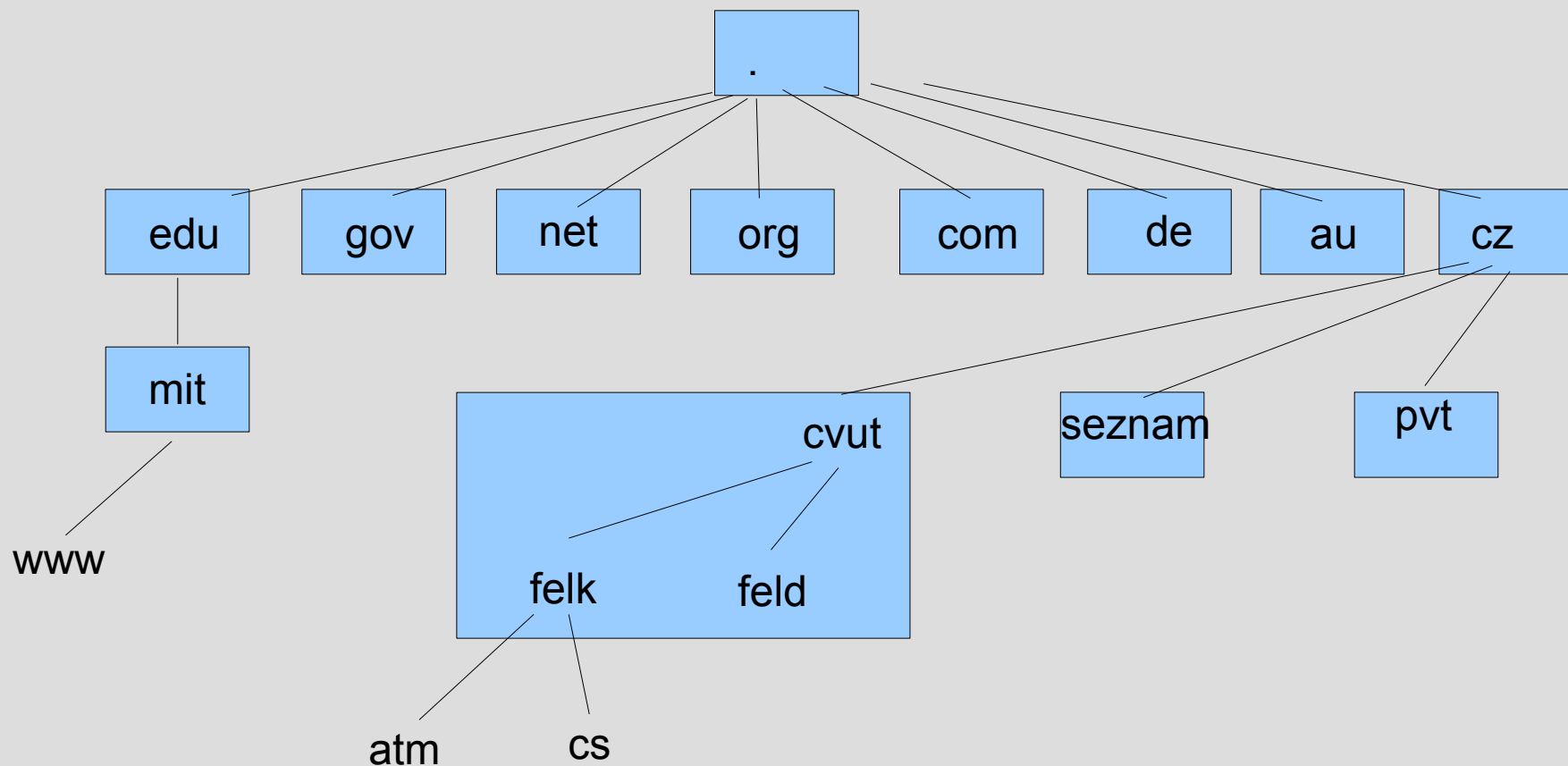
- pozitivní, negativní caching
- dns notify
  - informace sekundárním serverům o změně
- replikace primárního serveru
  - inkrementální zone transfer
- autentizace

# DNS dotaz

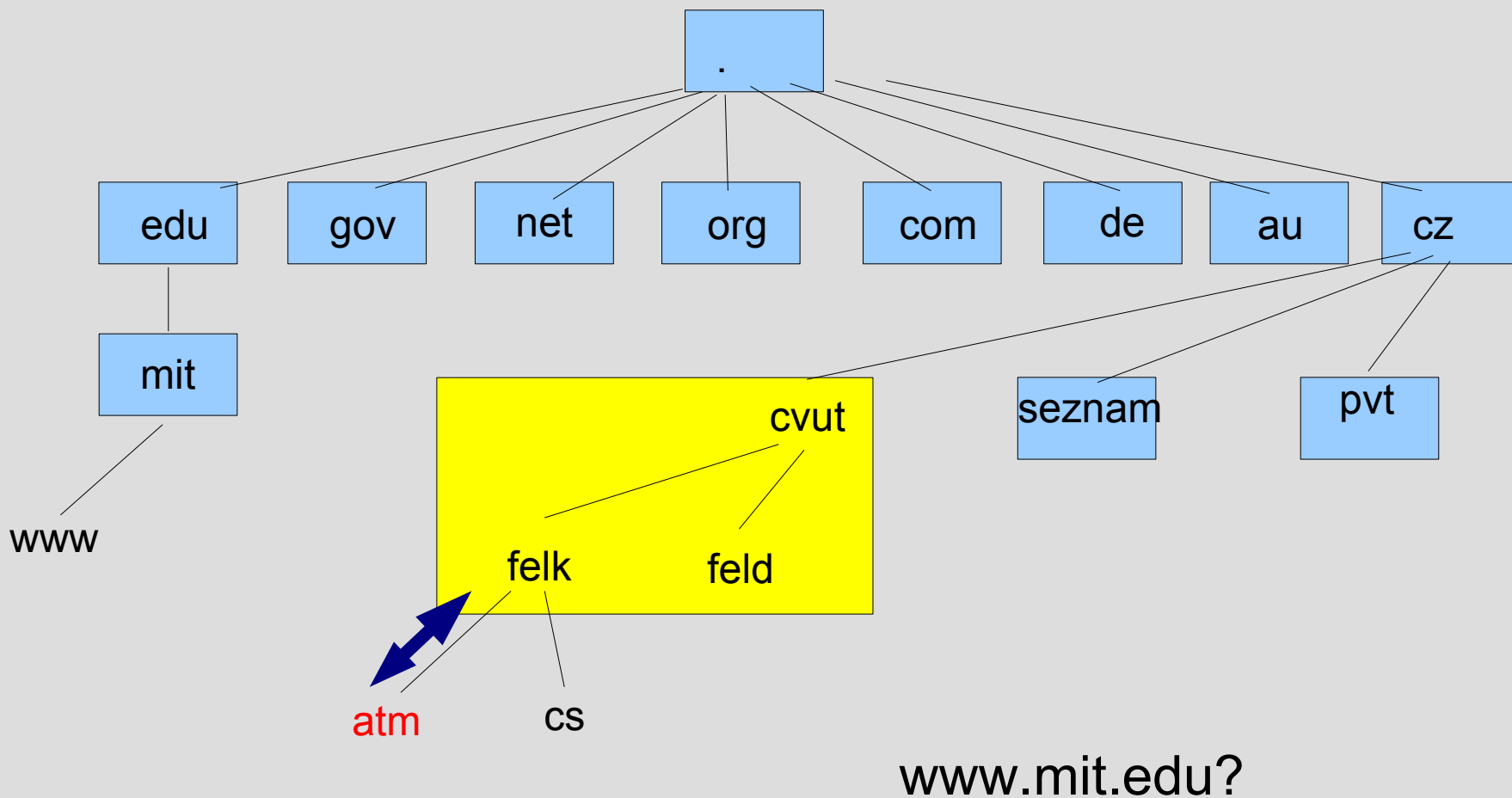
- může být zodpovězen autoritativně i neautoritativně
- pokud server nezná odpověď – obrací se na **root** **servery** a potom postupuje směrem k subdoménám podle NS záznamů
- může být vyžadován UDP checksum
- omezení UDP odpovědi na 512B
- obsahem odpovědi je i doba platnosti



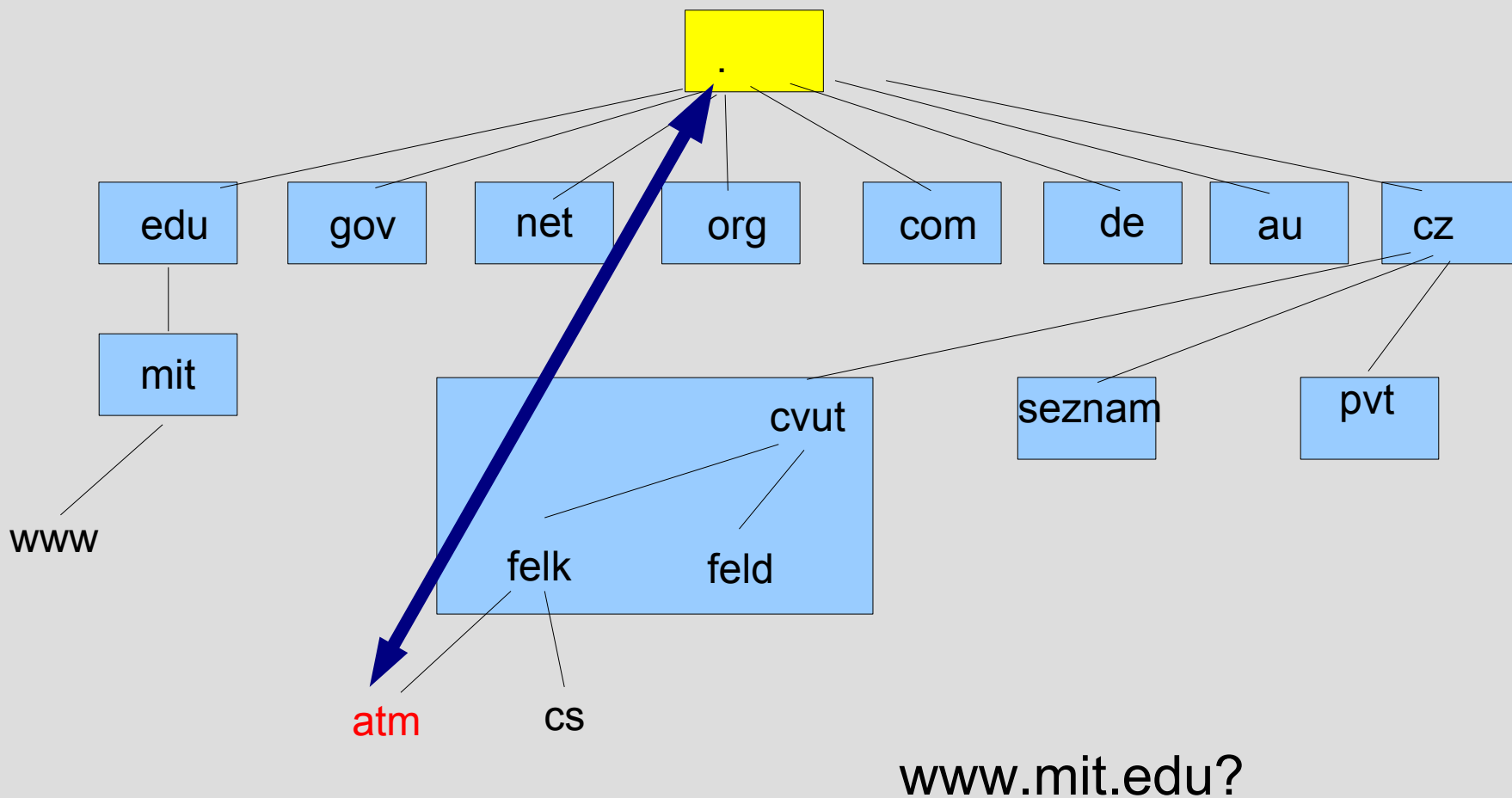
# DNS dotaz



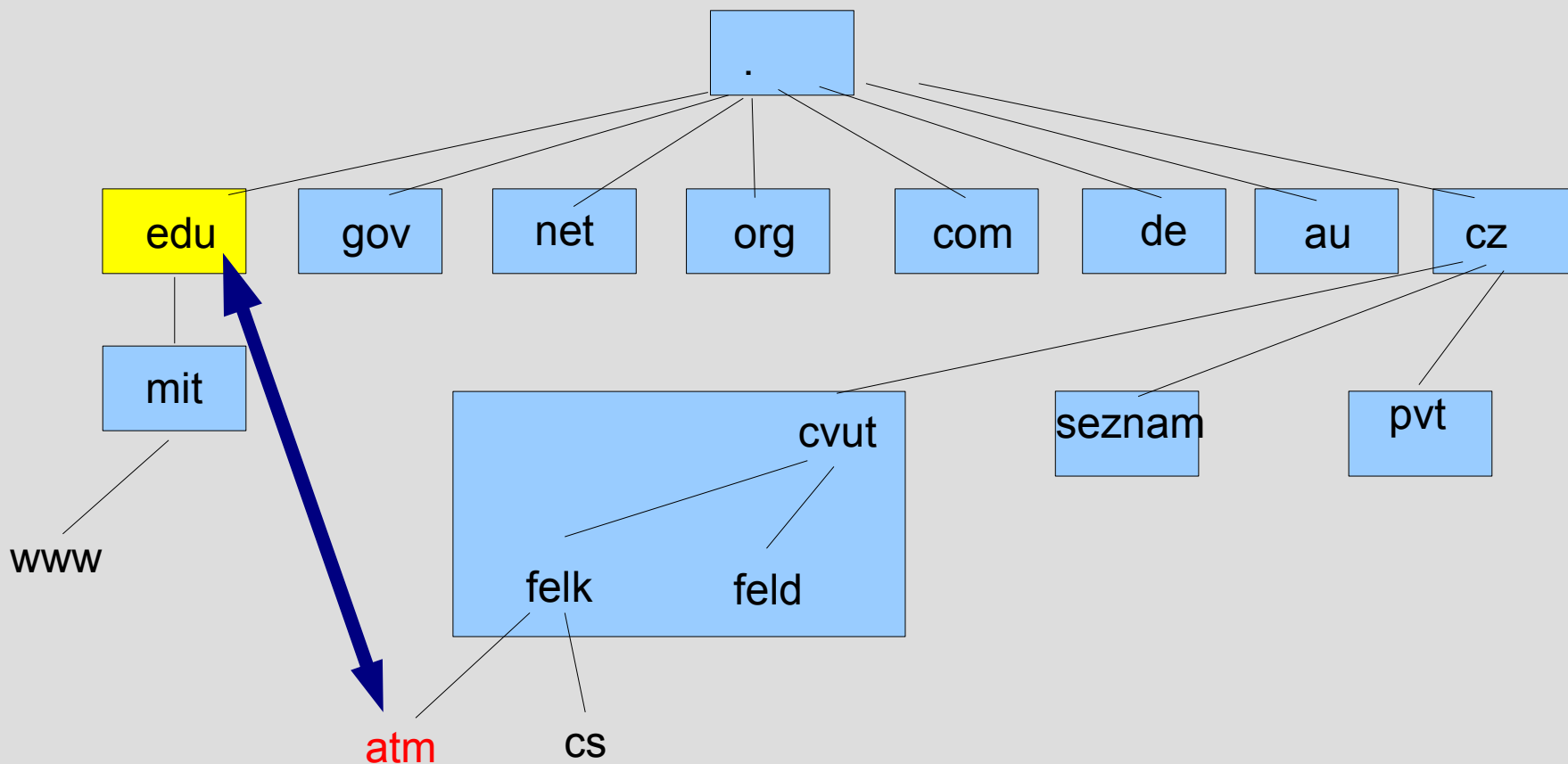
# DNS dotaz - nerekurzivní



# DNS dotaz - nerekurzivní

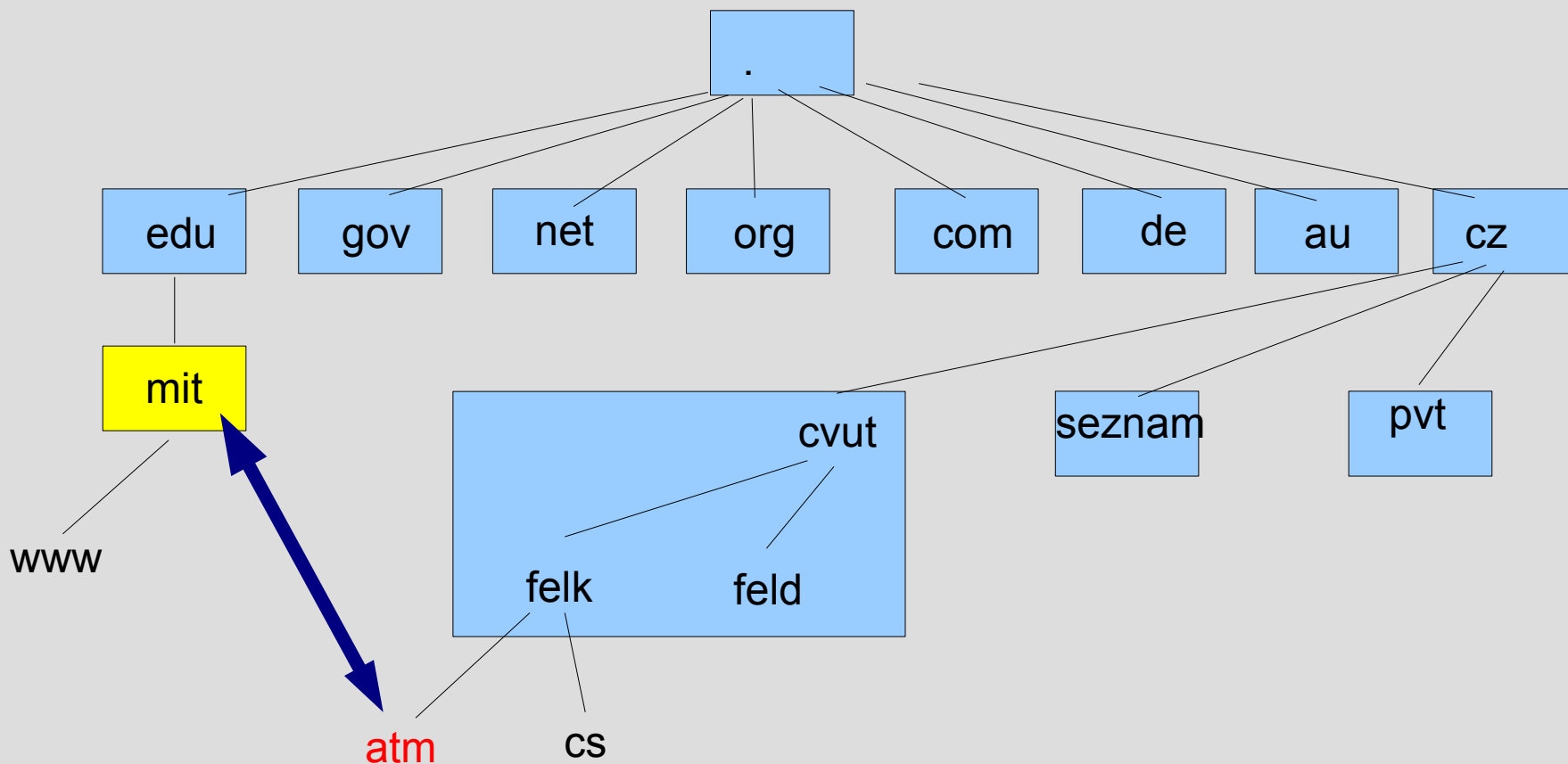


# DNS dotaz - nerekurzivní



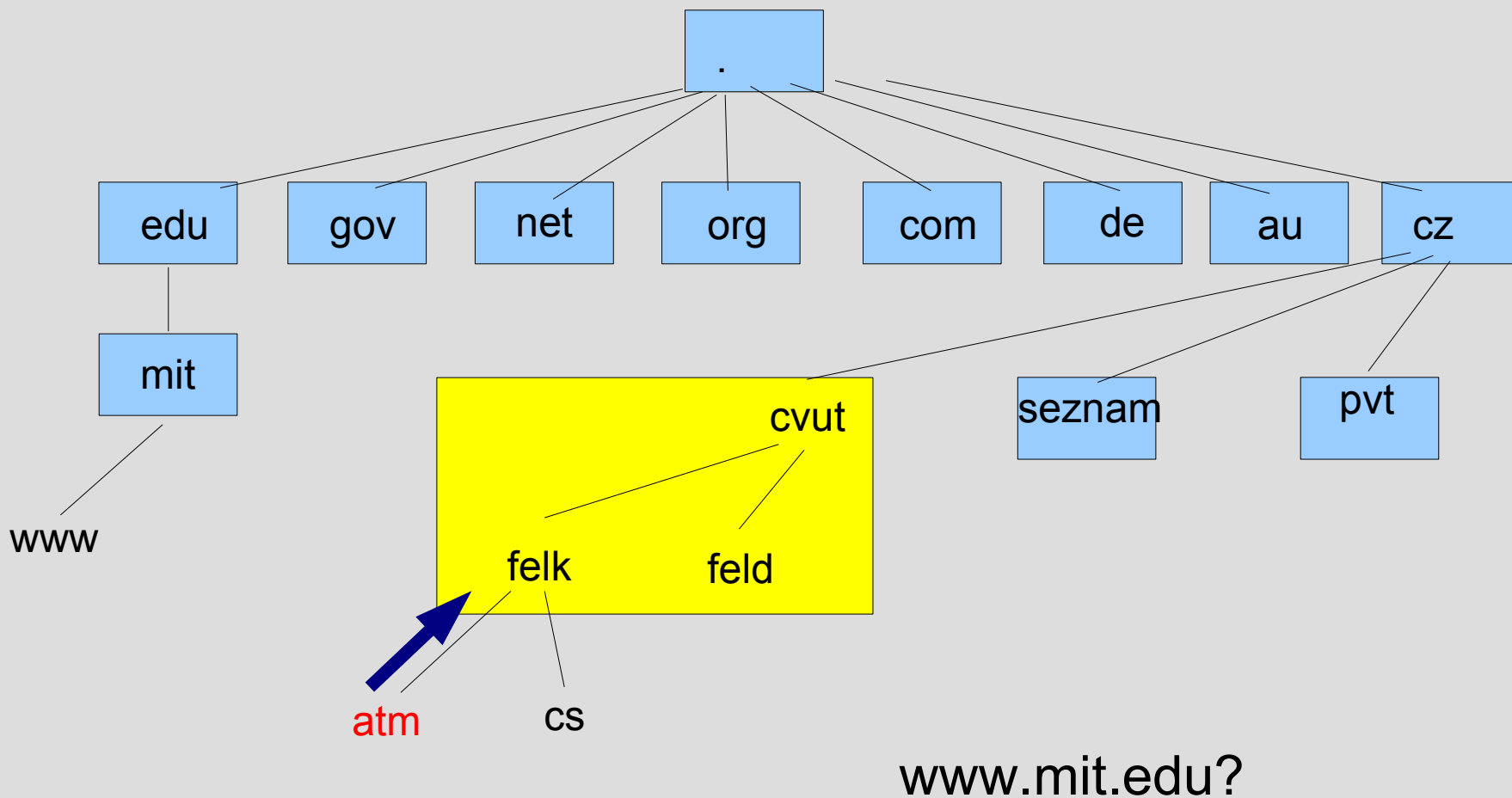
www.mit.edu?

# DNS dotaz - nerekurzivní

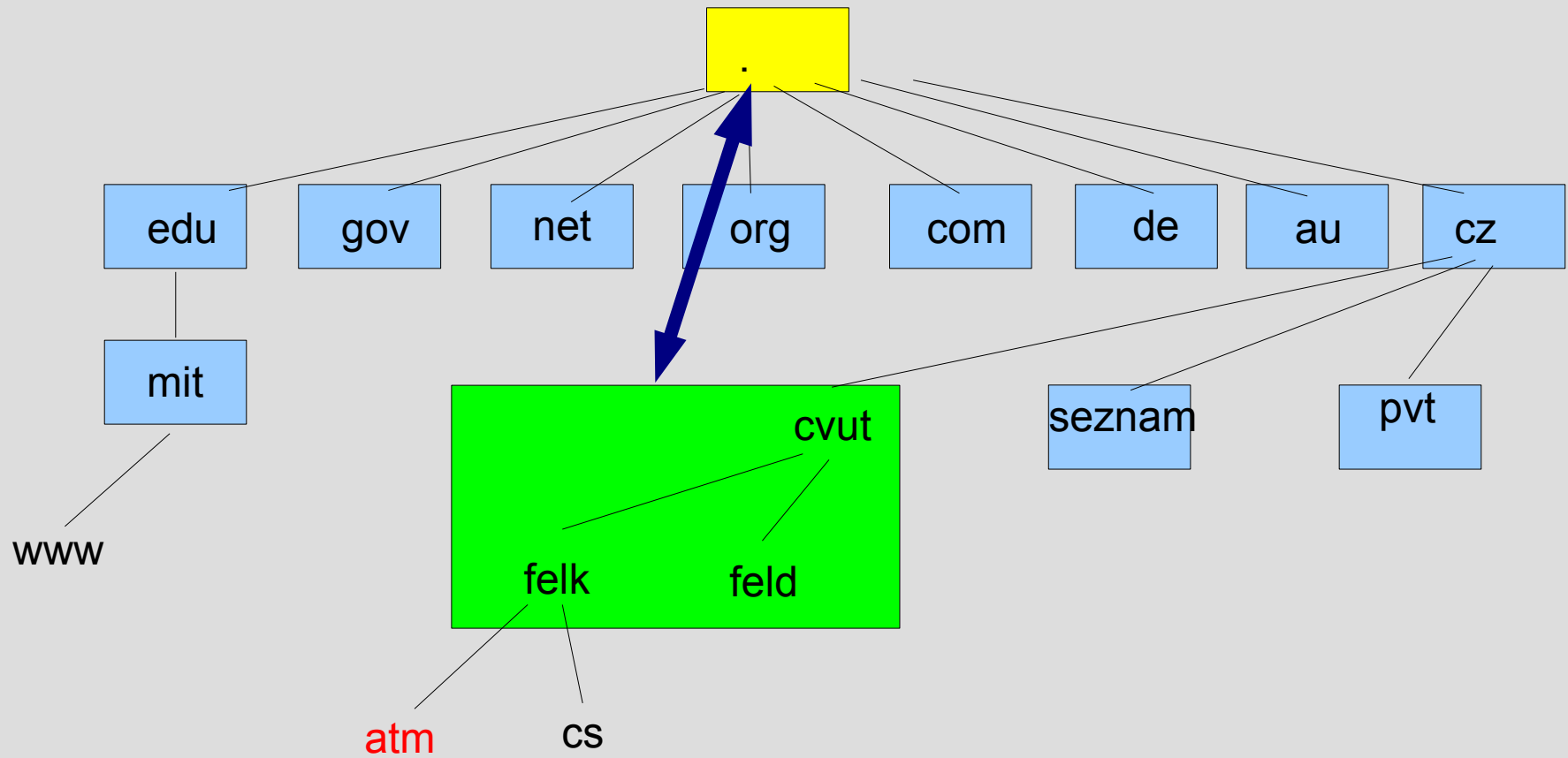


www.mit.edu=18.7.22.83

# DNS dotaz - rekurzivní

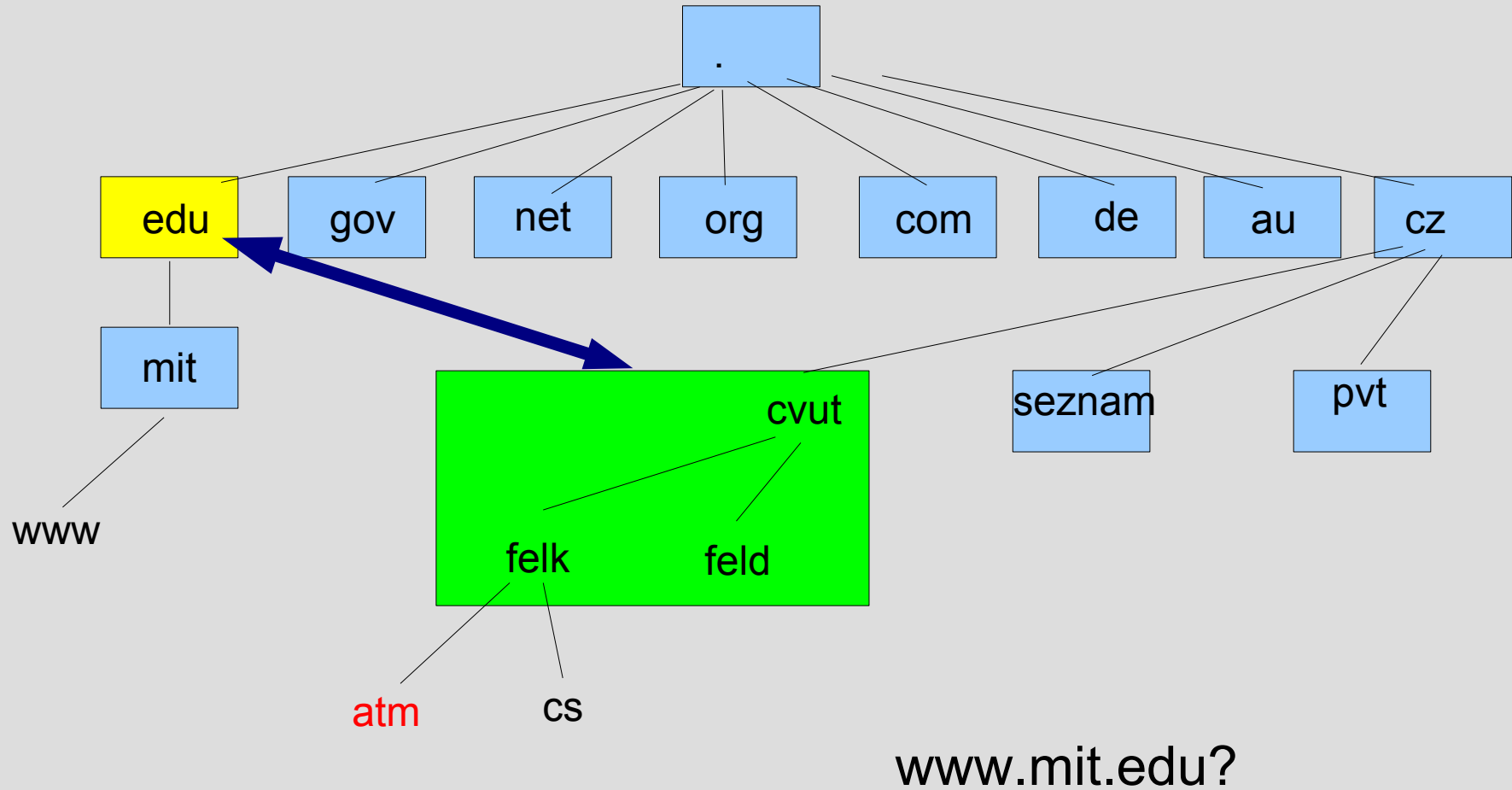


# DNS dotaz - rekurzivní



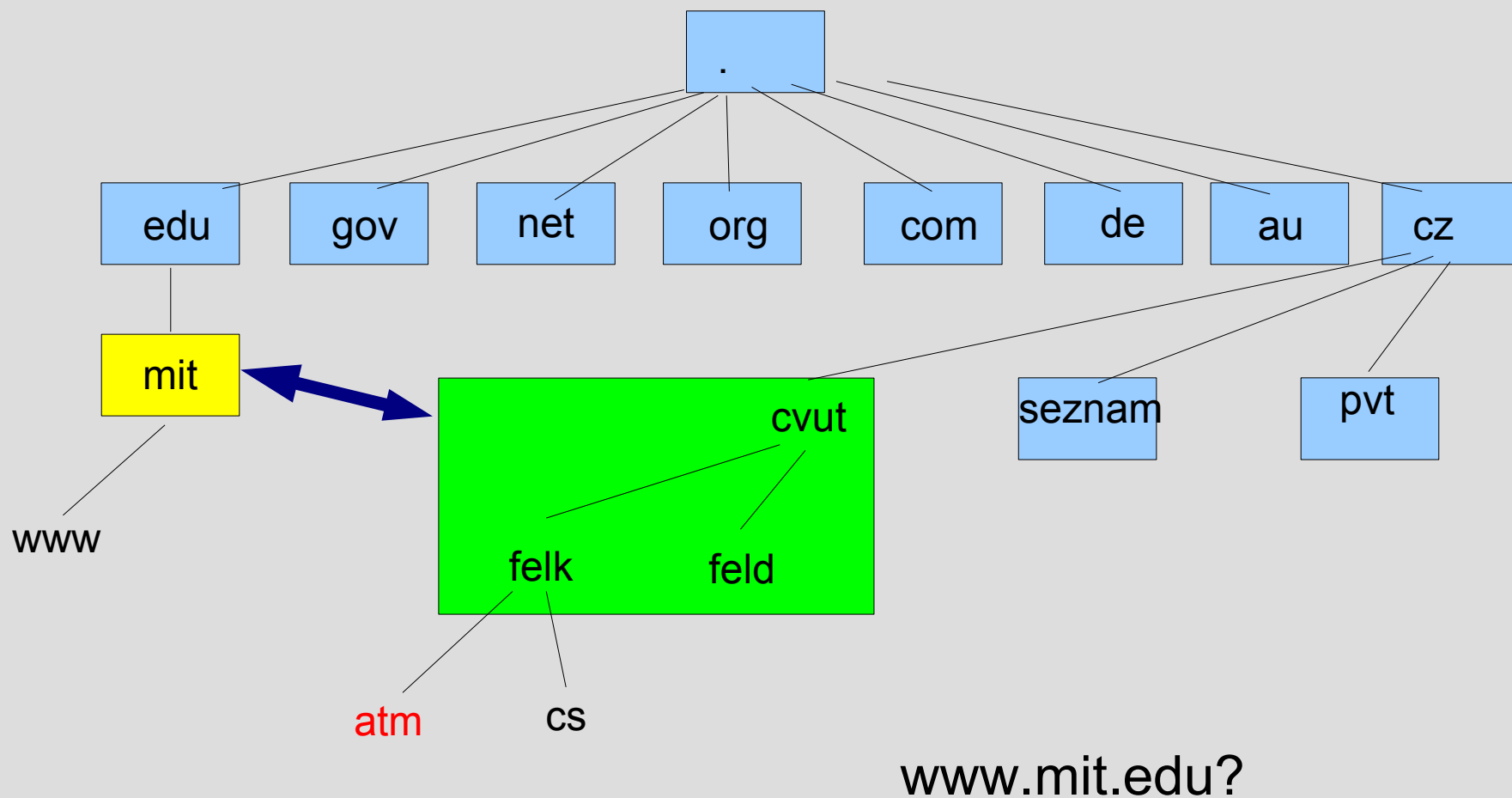
www.mit.edu?

# DNS dotaz - rekurzivní

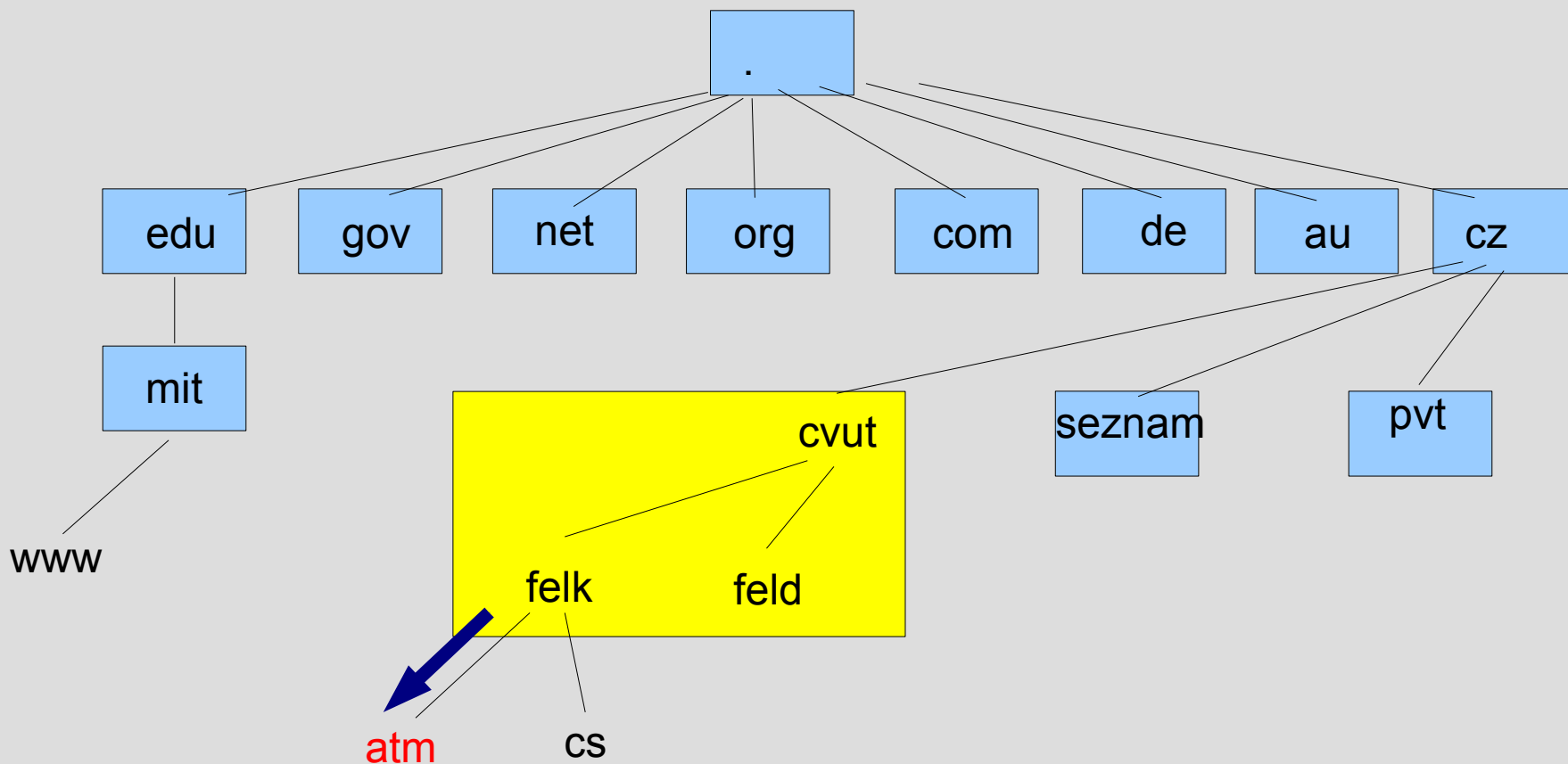




# DNS dotaz - rekurzivní

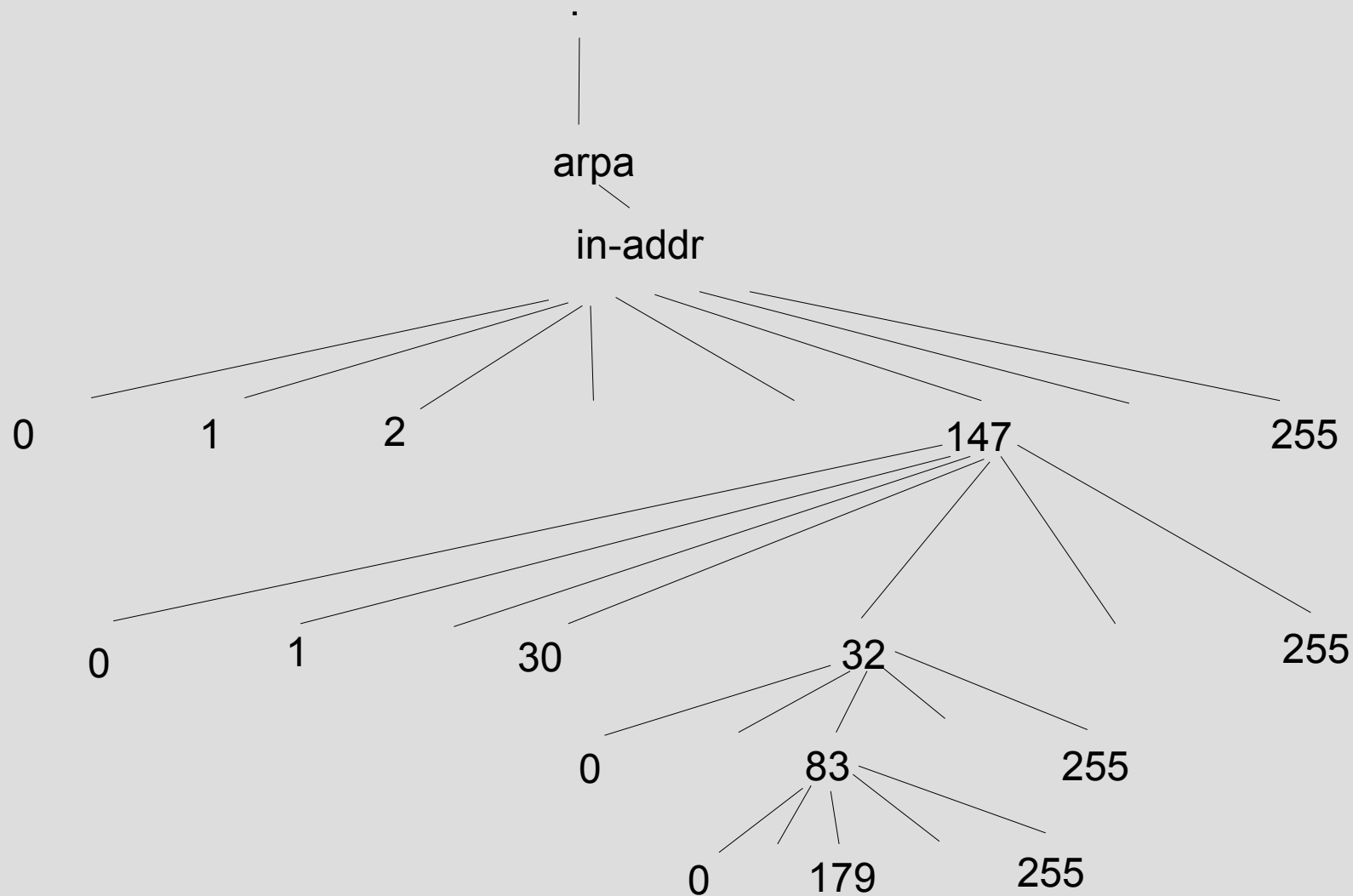


# DNS dotaz - rekurzivní

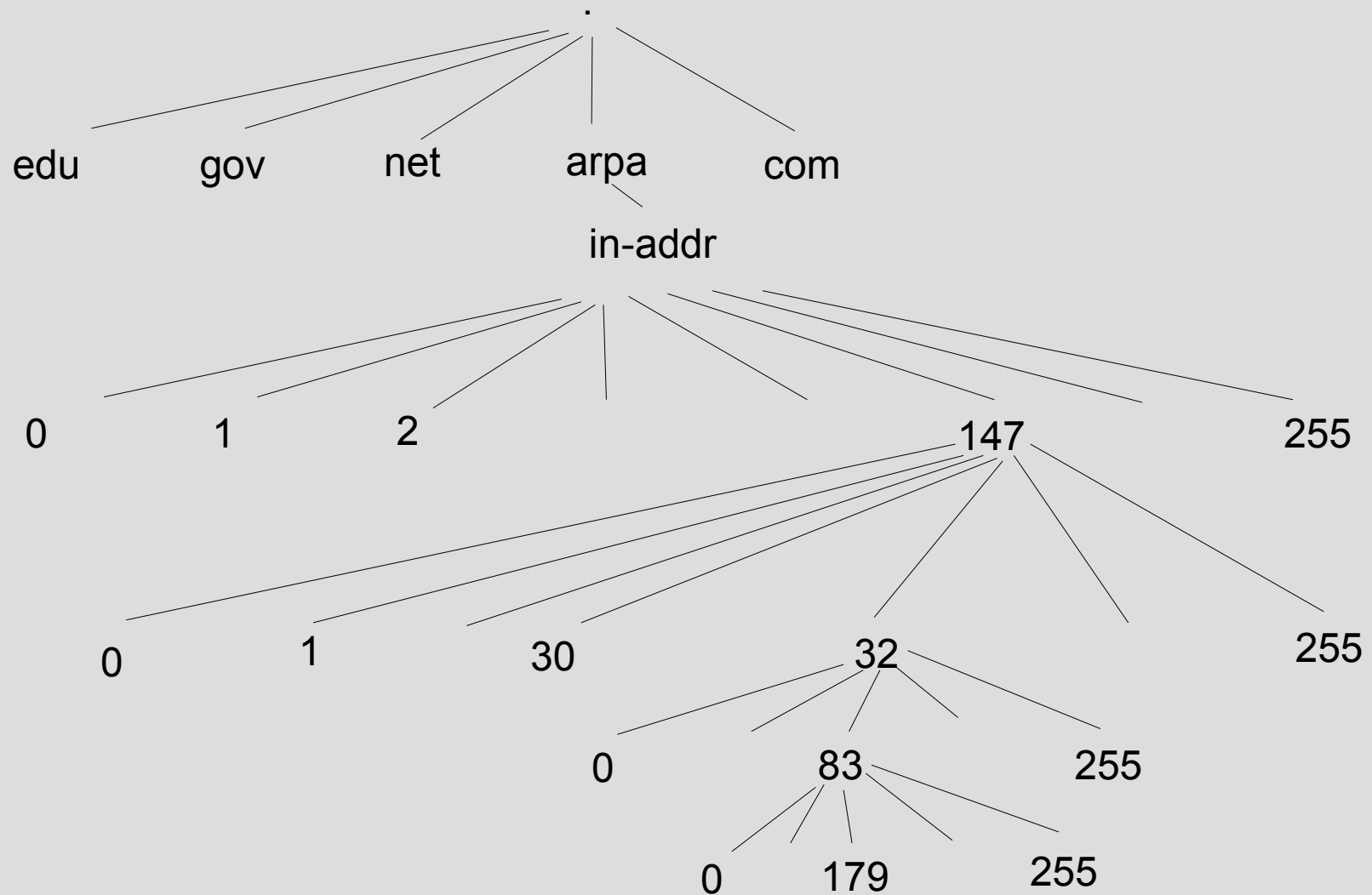


www.mit.edu=18.7.22.83

# Reverzní dotaz



# DNS reverzní doména



# Kombinace služeb

- integrace různých služeb v distribuovaném prostředí
- kombinace jmenné služby s portmapem
- DCE RPC, SUN RPC, JAVA RMI, CORBA ....

# Zajímavé odkazy

- <http://www.cesnet.cz/doc/techzpravy/2000-4/>
  - Technická zpráva CESNET – Adresářové služby
- <http://www.earchiv.cz/a909s200/a909s200.php3>
  - seriál o hledání na Internetu Jiřího Peterky



dsn

???