Directory services
Domain name services

Ing. Yelena Trofimova

Department of Computer Systems
Faculty of Information Technology
Czech Technical University in Prague

Computer networks, BIE-PSI
SS 2020/21, Lecture 9

`https://courses.fit.cvut.cz/BIE-PSI/`

Content

- the role of name (directory) services
- name services
  - X.500 and LDAP
  - DNS
    - DNS communication
    - root nameservers
    - recursive/non-recursive DNS request
    - reverse DNS

The role of name services

- specialized database
- address book
  - reading and search optimization
  - occasional updates
  - distribution
  - replication
  - no transaction support
- tasks
  - translation
  - check
  - search (localization)
  - providing detailed information (features)

Name services

- files
- X.500
- LDAP – Lightweight Directory Access Protocol
- DNS – Domain Name System
- NIS – Network Information Service
- MS Active Directory
- and others

X.500

- CCITT X.500 - X.521
  - 1988 - ISO 9594
- hierarchical namespace
- client-server communication
  - Directory Access Protocol (DAP)
    - OSI protocol
  - Lightweight Directory Access Protocol (LDAP)
    - TCP/IP, skipped functions, does not define a directory
    - originally just an X.500 server access protocol
    - LDAP server was gradually created
- decentralized, unified global space, support of arbitrary attributes, complex queries, authentication support, ACL

X.500 – data organization

- attribute – pair [name: value]
- record – one or more attributes
- Relative Distinguished Name – unique attribute within one directory level
- Distinguished Name – A sequence of all relative unique names from the root
- attributes (X.520)
  - C Country, SP State or Province, L Locality, O Organization, OU Organization Unit, CN Common Name

DNS

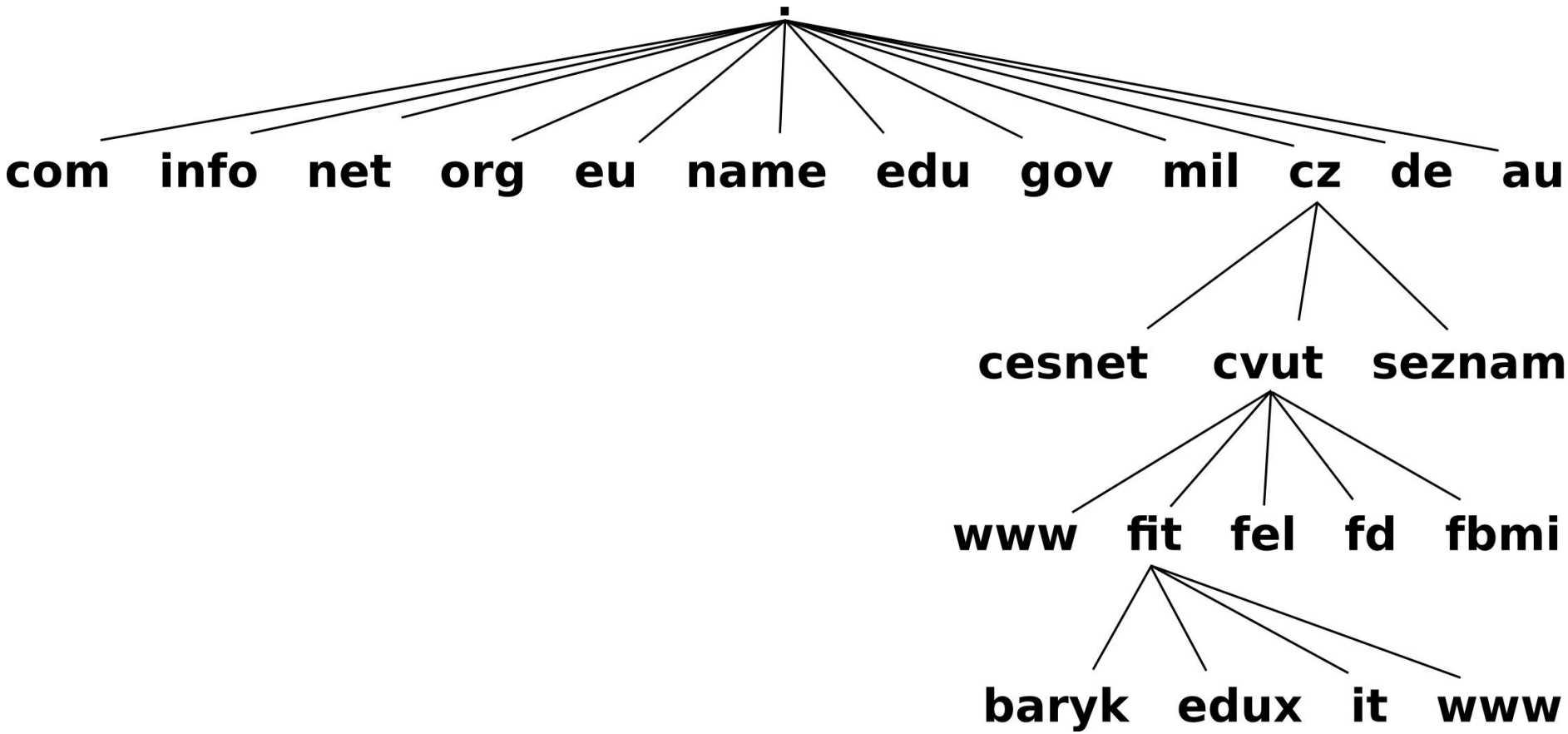
- Domain Name System – rfc1034, rfc1035
- primarily intended for name-to-address translation
- is based on the /etc/hosts file structure
- records:

A	32b IP Address
NS	authoritative name server
CNAME	synonym to name
SOA	start of authority
PTR	reverse translation
HINFO	SW and HW description
MX	preference and mail server name
TXT	text string
AAAA	128b IP Address
...	

DNS components

- namespace and source records
  - tree structure
  - name 0 - 63 B, total max 255 B
  - absolute name (eg. edux.fit.cvut.cz.)
  - relative name (eg. edux)
- name servers
  - data warehouses creating a name database
  - answer questions
  - synchronize the database
  - maintain the response cache
- resolvers
  - a set of library functions providing translation

DNS domains


.
com
info
net
org
eu
name
edu
gov
mil
cz
de
au
cesnet
cvut
seznam
www
fit
fel
fd
fbmi
baryk
edux
it
www

DNS – types of servers

- primary
  - keeps zone data
  - authoritative server
- secondary
  - copies data from the primary server
  - authoritative server
- caching only
  - is not authoritative for any zone
- root
  - maintains root domain records
- forwarding
  - passes a recursive query (link relief), also can resolve by itself

DNS – communication I

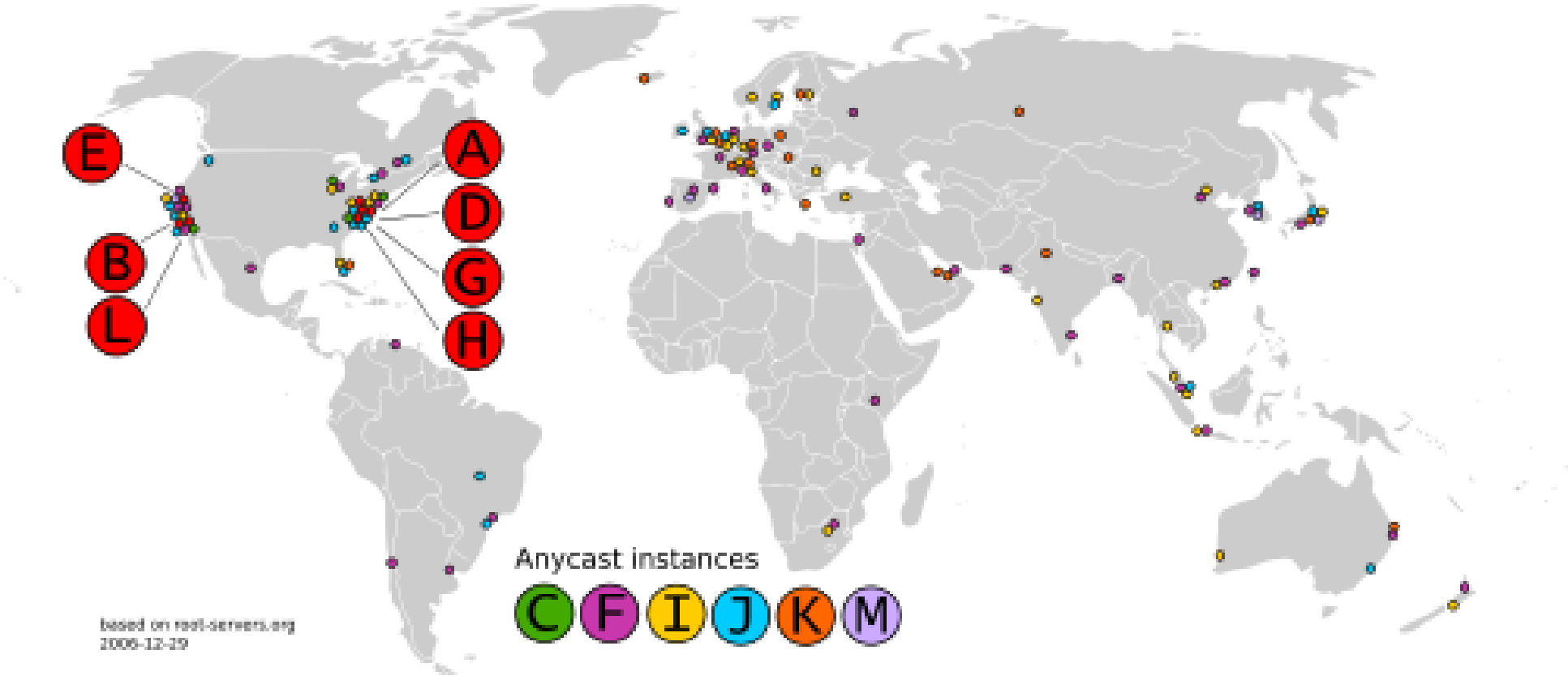
- both TCP and UDP
- port 53/udp, 53/tcp
- query - UDP up to max. 512B, otherwise TCP
- zone transfer - TCP
  - the query is sent to multiple servers
  - the first answer is valid, the others are discarded
  - nameserver inconsistency
- dns query, dns answer
  - recursive/non-recursive query and answer

DNS – communication II

- dns update
  - support for ddns; zone information, assumptions, update
- dns notify
  - information for secondary servers about change
- primary server replication
  - incremental zone transfer
- authentication

DNS root nameservers

As of 2020-01-11, the root server system consists of 1034 instances operated by the 13 independent root server operators.

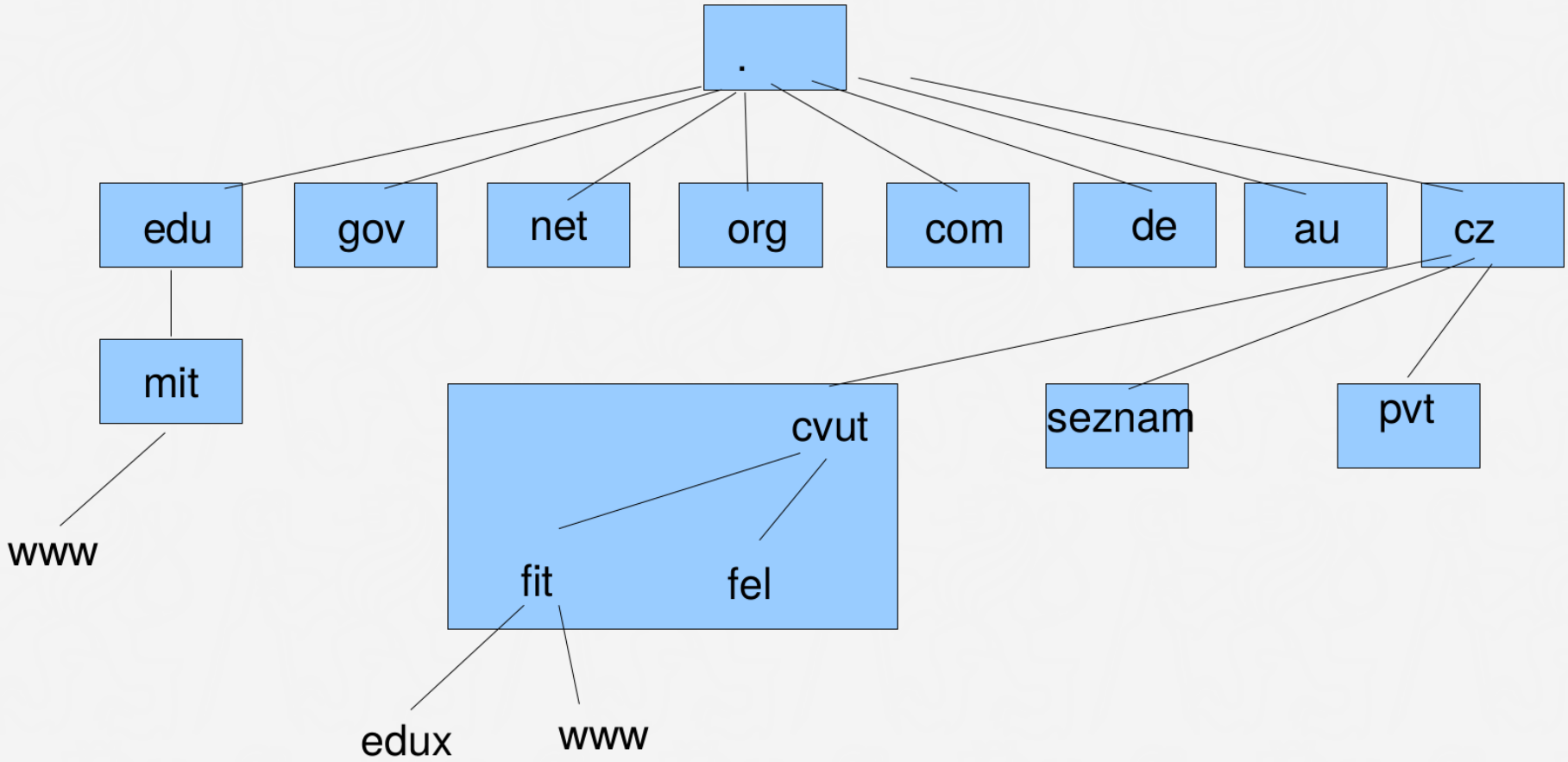


DNS root nameservers: A – M, top-level domain

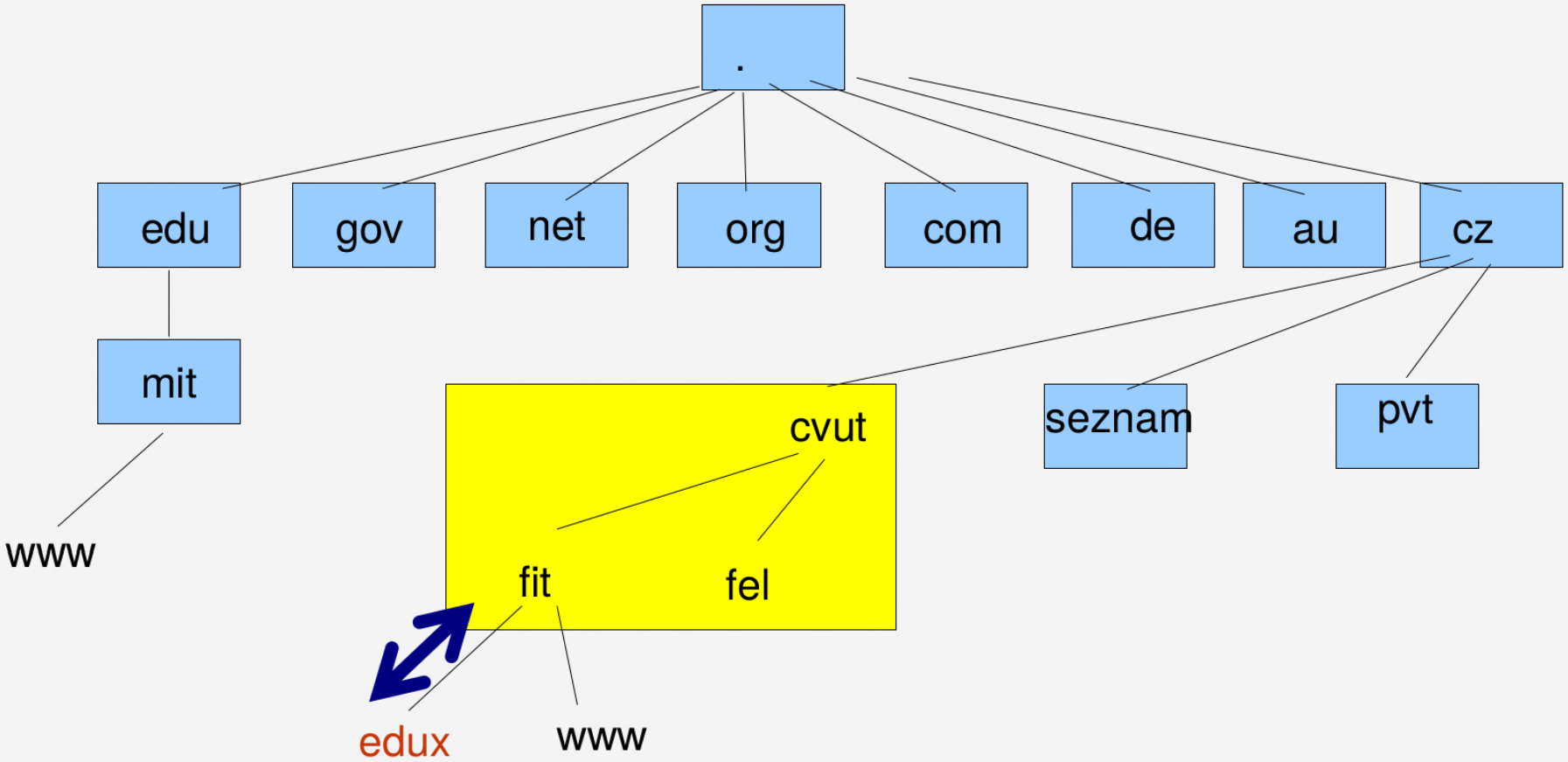
DNS request

- the query can be answered both authoritatively and non-authoritatively
  - usage of cache
- if the DNS server does not know the answer
  - recursive behavior: finds the answer and tells the source of the request
    - send request to root servers and then proceed towards subdomains according to NS records
    - typical behavior of local DNS servers
  - non-recursive behavior: not looking for an answer
    - forward the requester the IP address of the DNS server to be asked
    - typical for higher-level DNS servers (i.e. closer to top level)
- the source may request recursive server behavior, server it may refuse

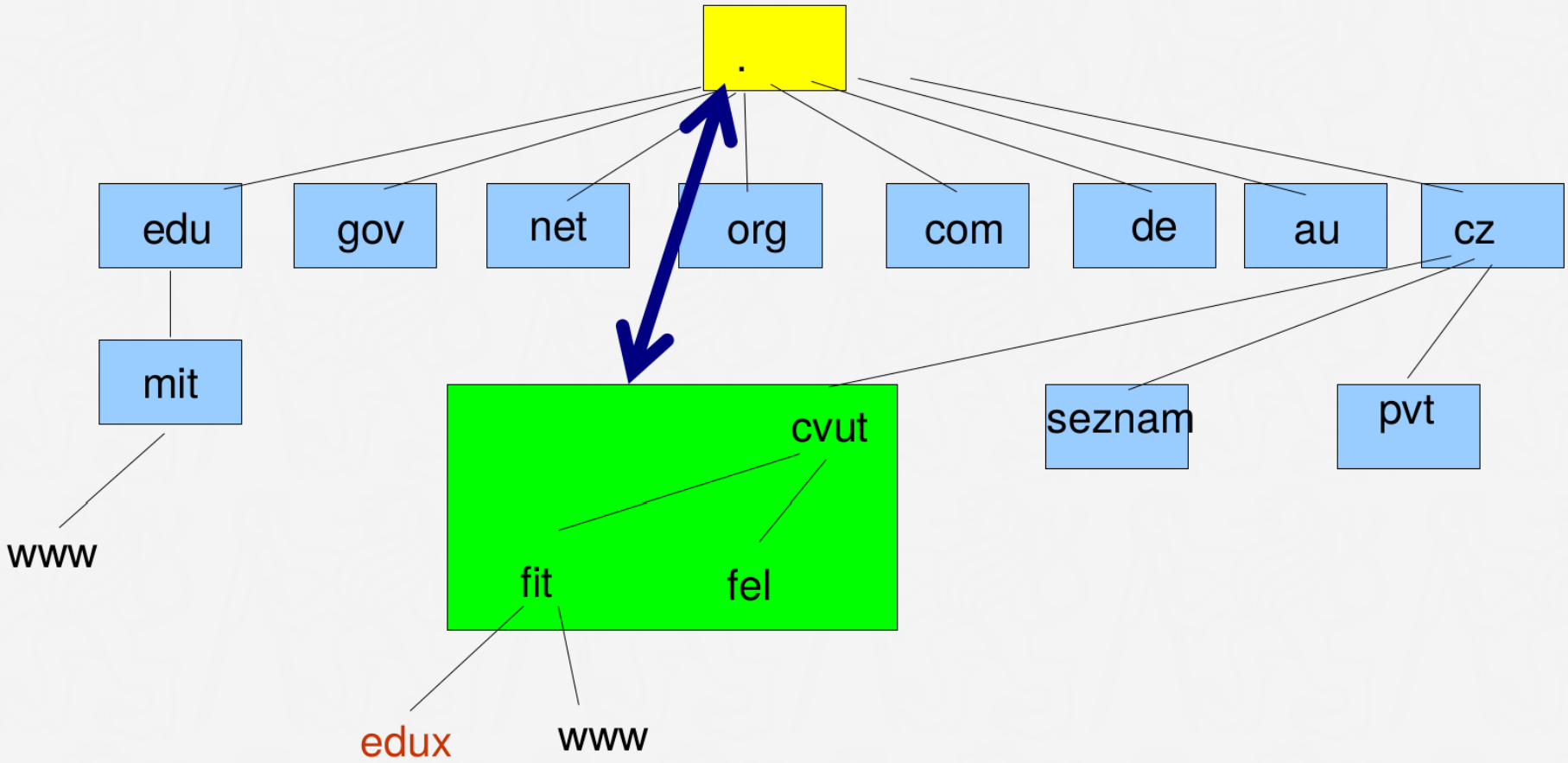
DNS request – example



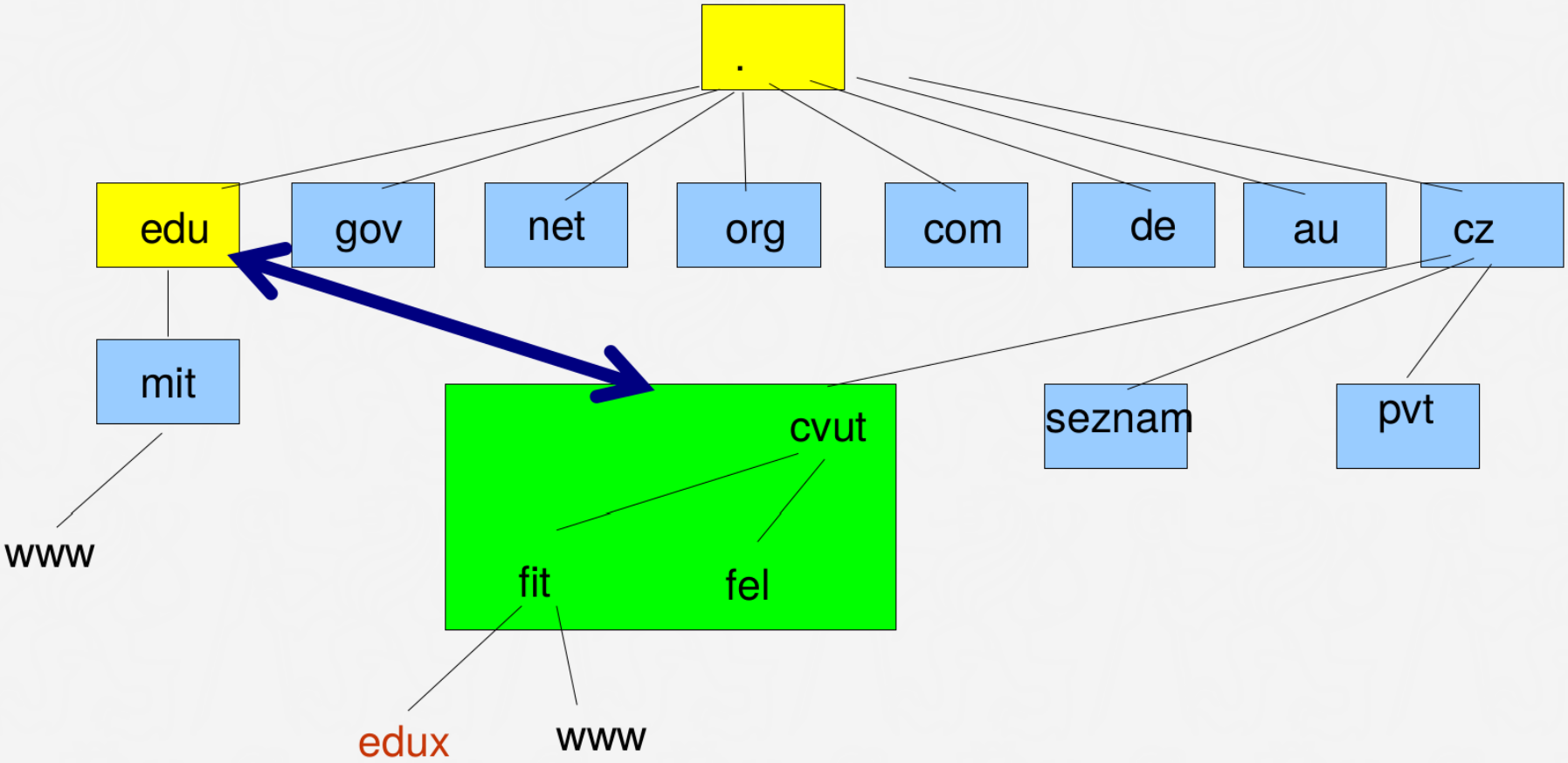
DNS request – recursive I



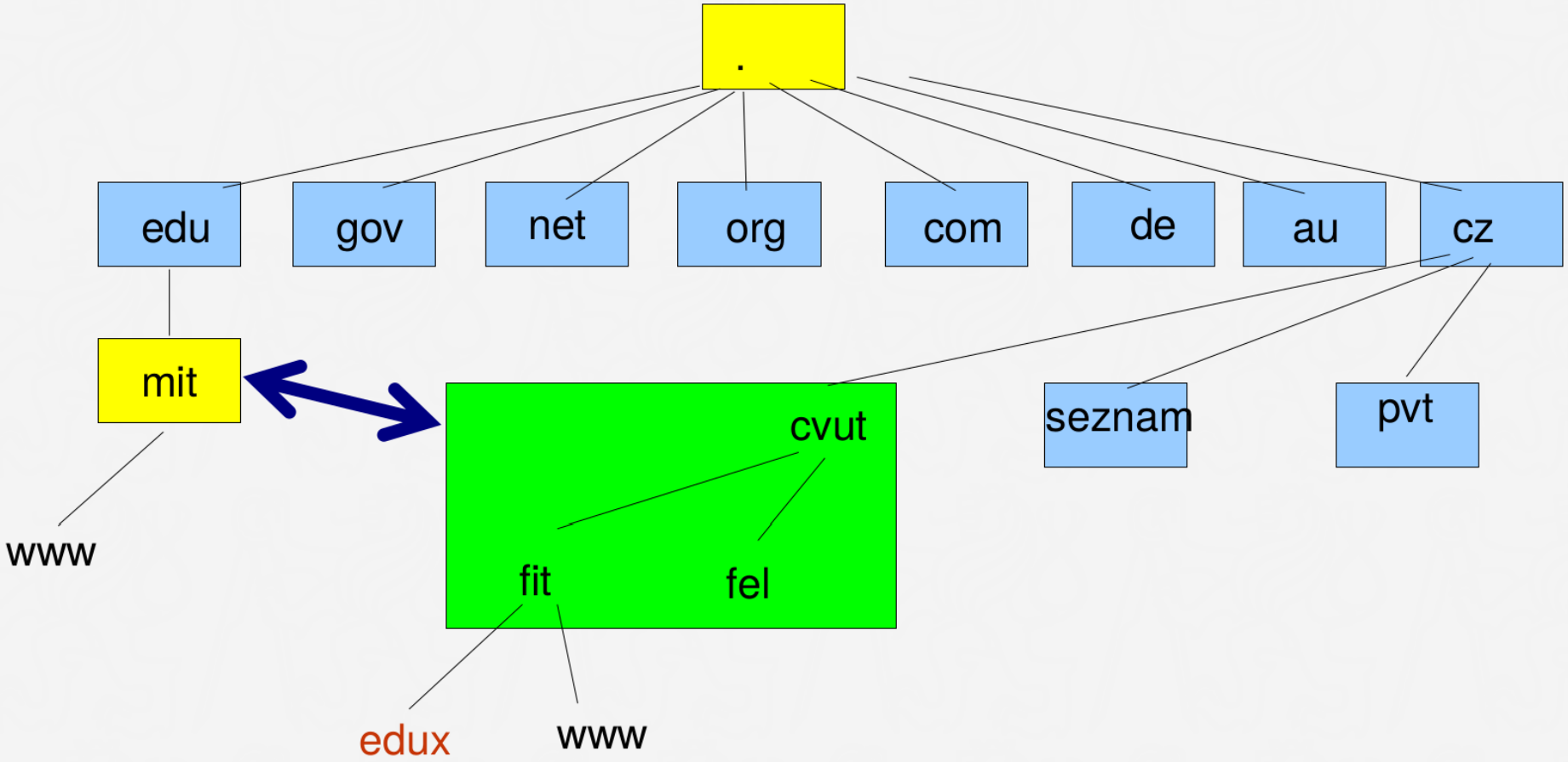
DNS request – recursive II



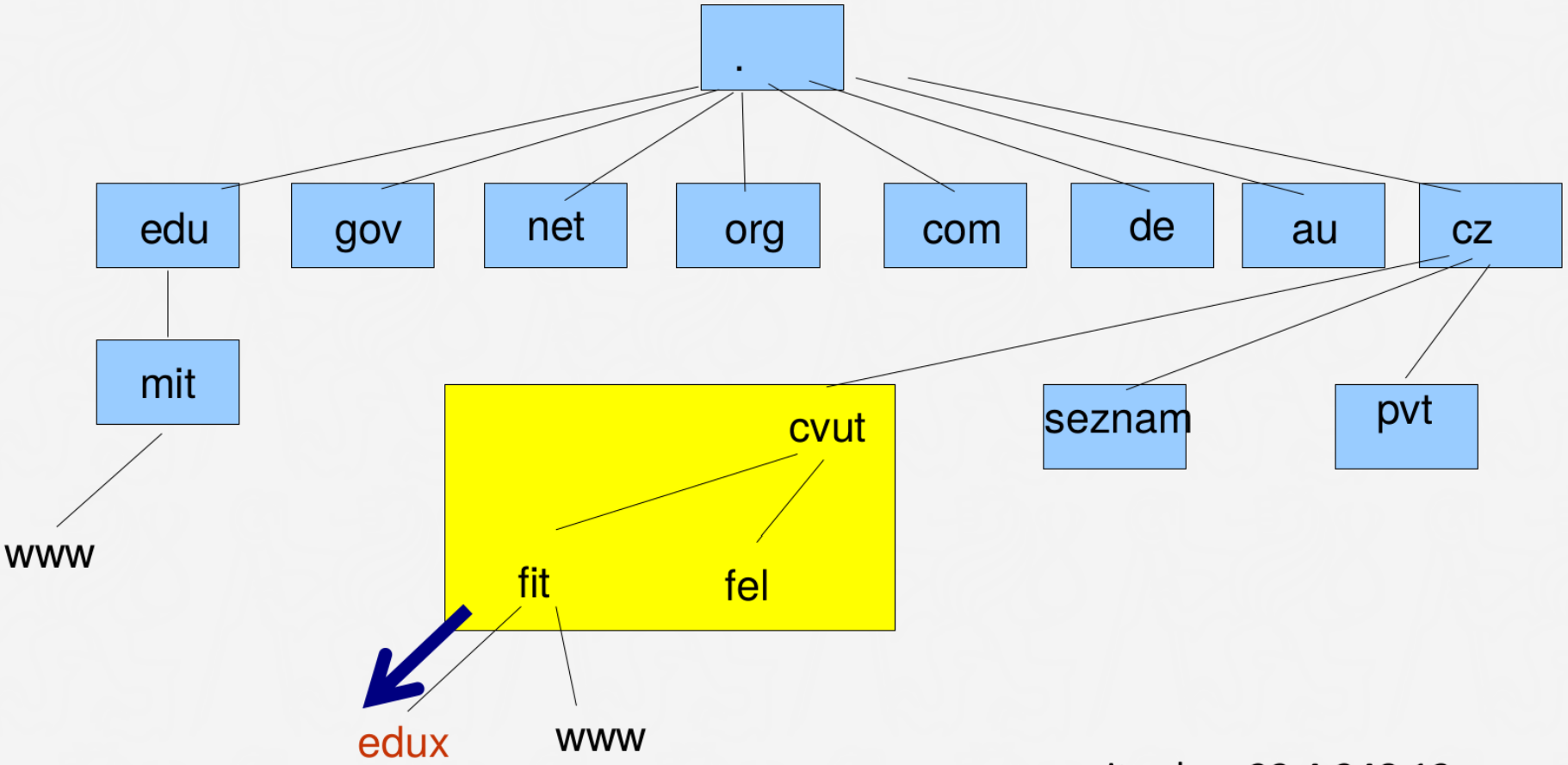
DNS request – recursive III



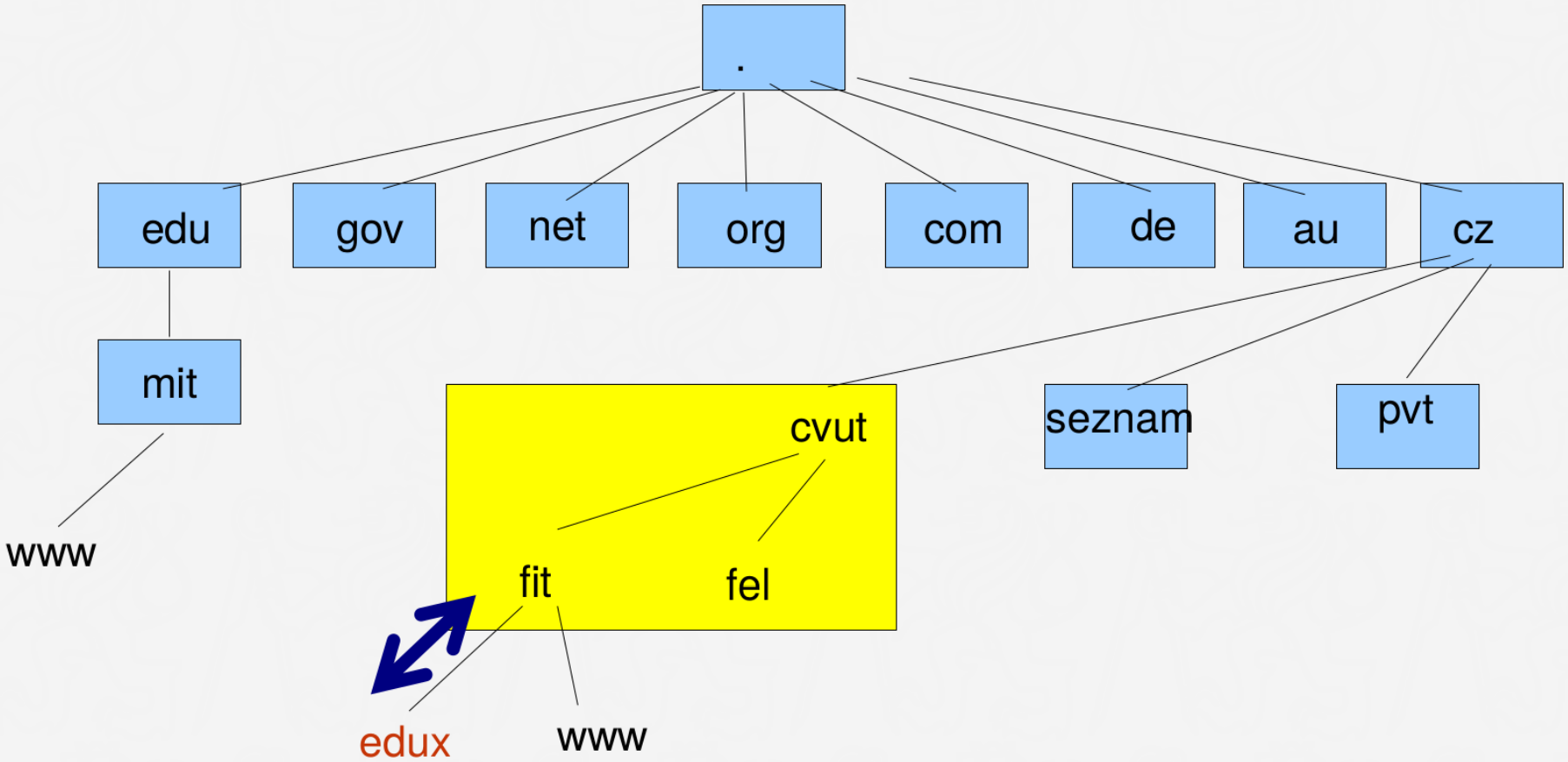
DNS request – recursive IV



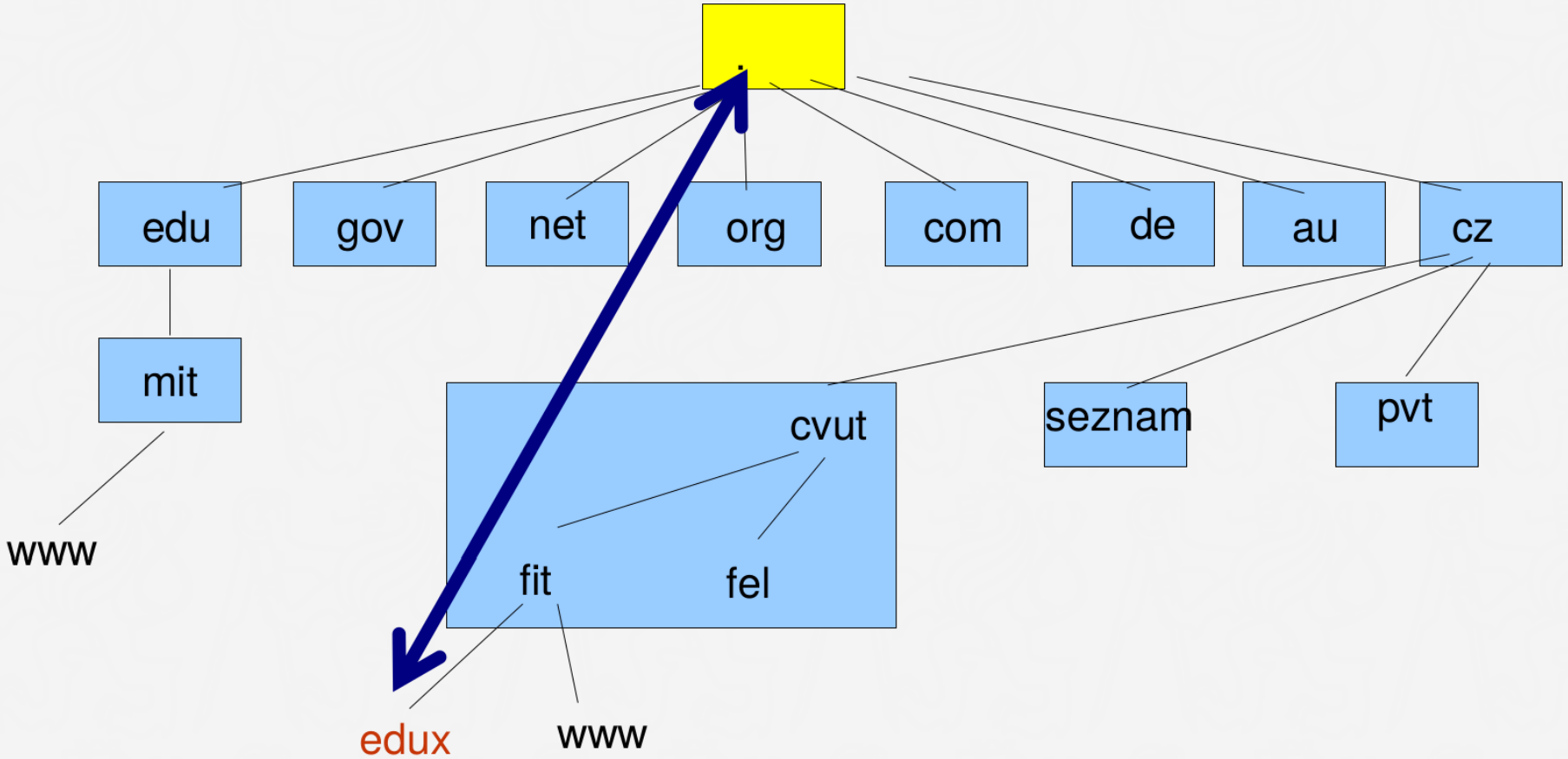
DNS request – recursive V



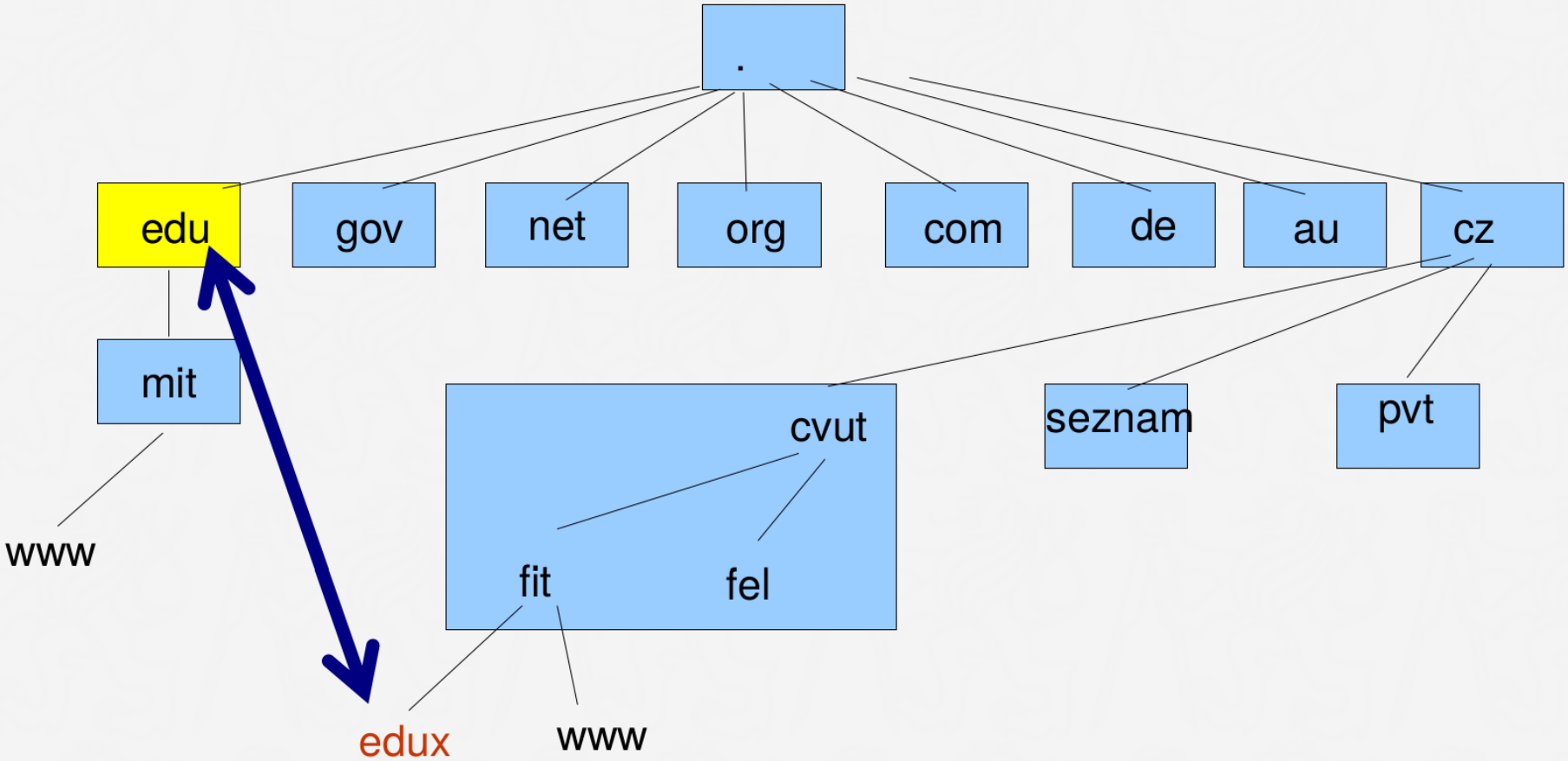
DNS request – non-recursive I



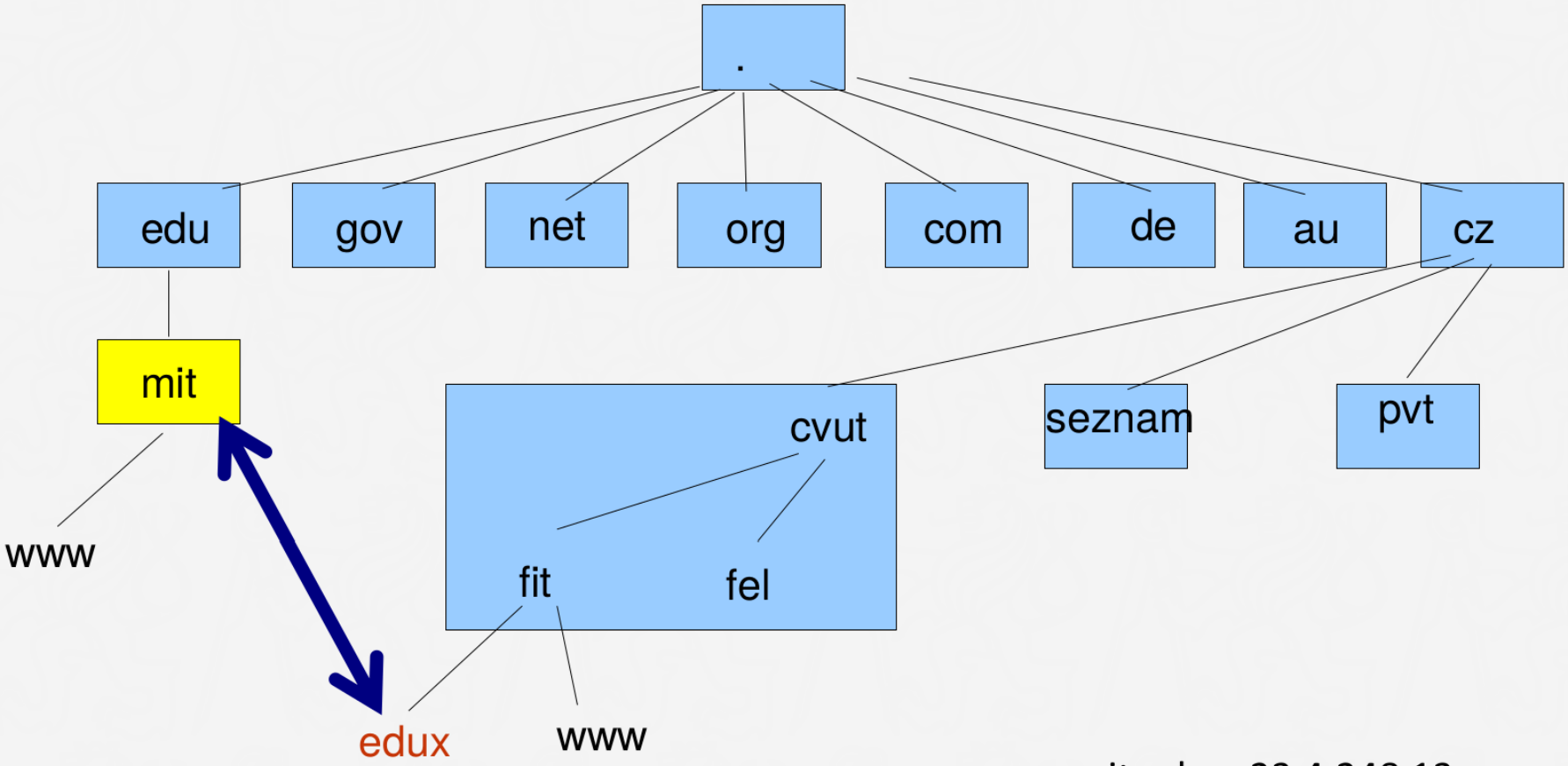
DNS request – non-recursive II



DNS request – non-recursive III



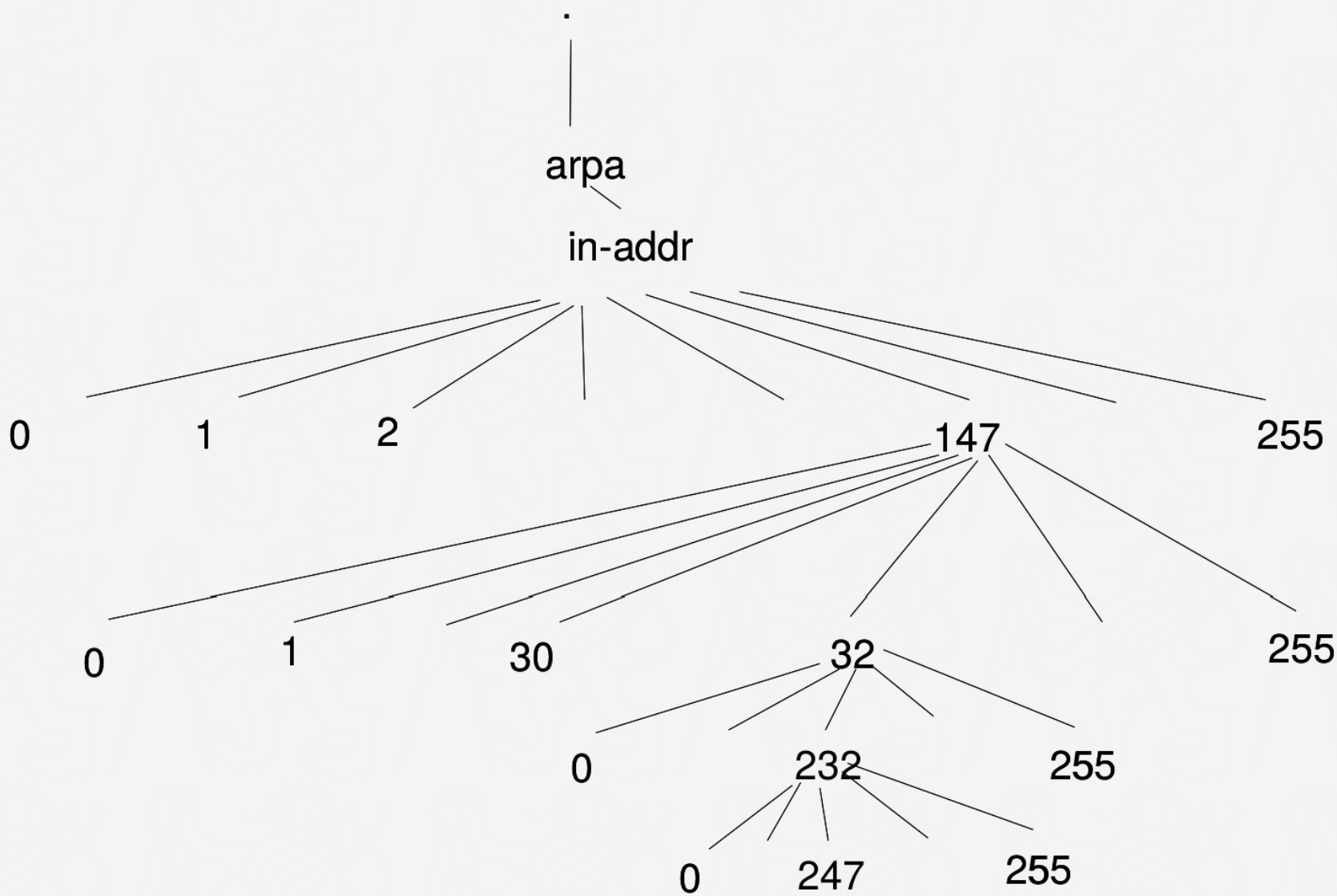
DNS request – non-recursive IV



Recursive/Non-recursive comparison

Source: steves-internet-guide.com

Reverse DNS request



Reverse domain