$18.12 \rightarrow 16^{30}$ $1.5 h$

(so 2×45 min.)

$07.12 \rightarrow 16^{00}$ 3×45 min.

$1\frac{1}{2}.12 \rightarrow 16^{00}$ 3×45 min.

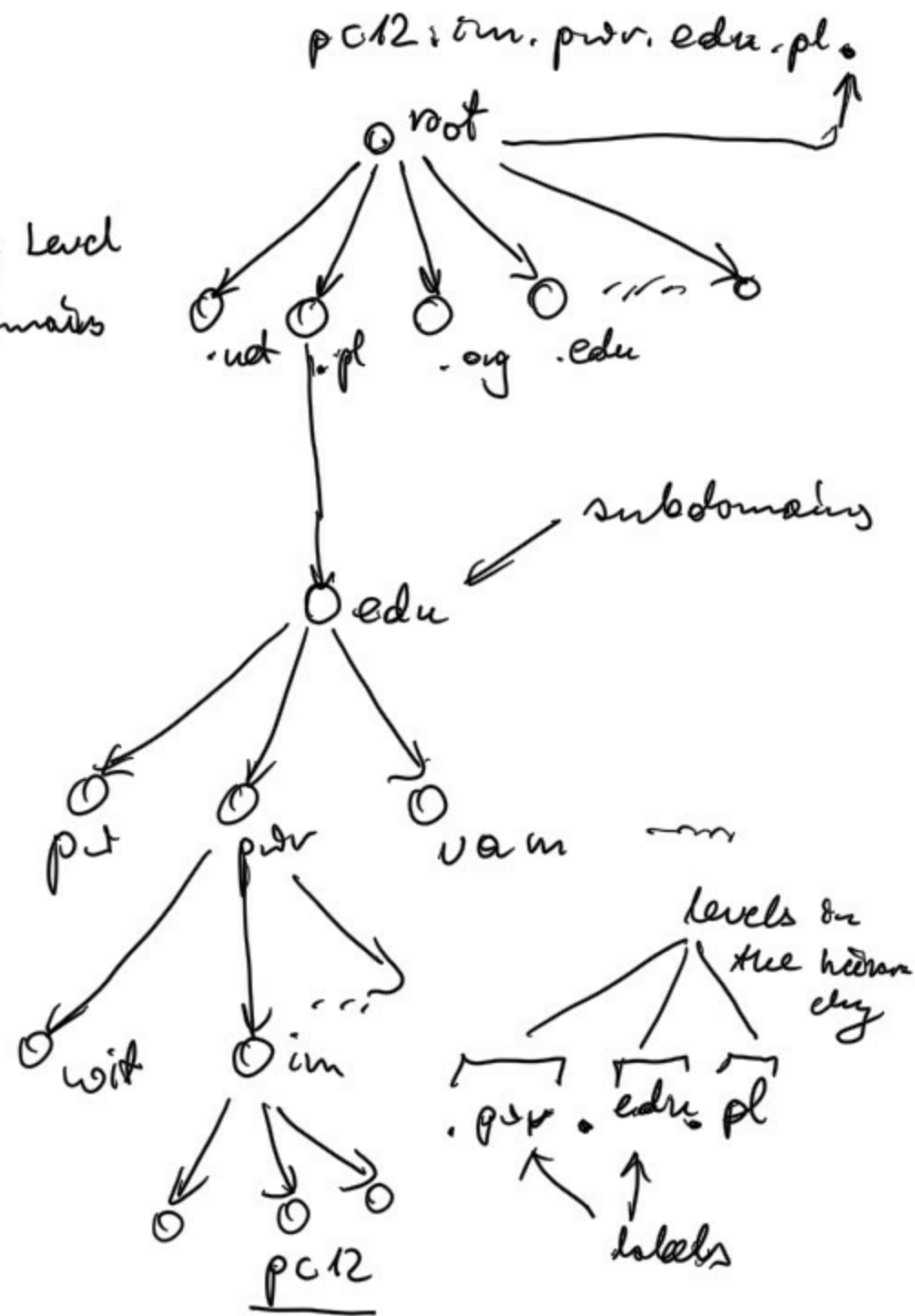# DNS (SEC) — introduction

DNS: translates human readable
address to an IP address

$pc12.im.pwr.edu.pl \rightarrow$ IP

biblioteka.im.uwr.pl
           edu

How the name system is organized?

We have a global tree:

---

pc12.im.pwr.edu.pl.

Top Level
Domains

.net .pl .org .edu

subdomains

edu

pit   pwr   uam

wit   im

pc12

levels in
the hierar
chy

.pwr .edu .pl

labels

So if we read from the right
to the left we can identify unique

path to the host pc 12.

This full (absolute) path to the host is called a Fully Qualified Domain Name (FQDN)

~~Usually~~

How the client finds info about pc12?

1. A part of code of the client (e-mail client or a browser) is responsible to call the DNS service.
This client is called the resolver.
It contacts a DNS server indicated in network configuration (IP set manually or by DHCP).

local

iterative query referral

root DNS server

DNS (recursive server)

.pl

.edu .pl
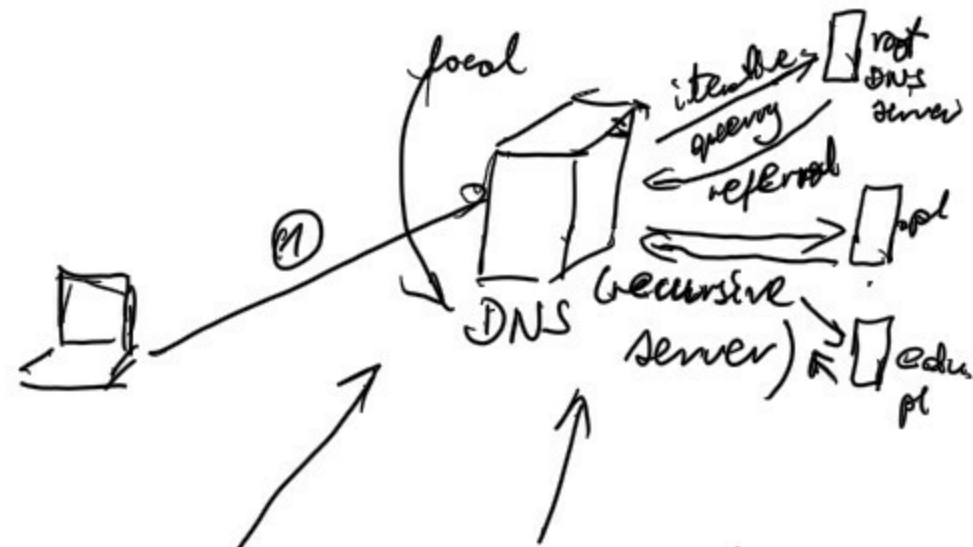
portal /entry-point to the global domain name system

recursive because the client expects that the server will find the answer even if it does not know it.
(so the server is able to send the request recursively)

2. The ② server will search its configured data files for the answer.
usually this server is responsible for some area (zone) – for such

an area it is authoritative – for example it may be a DNS server of a company.

3. If ② is not authoritative for the domain in question, the server will check the cache if the response for the same or similar query it there – if it finds the answer then responds with non-authoritative information and the process stops.
(The non-authoritative flag is set in the answer).

4. If there is no answer in the cache then escalation begins (② will contact another DNS server).

If info from the cache indicates a partial answer (from the left, e.g. uw.edu.pl was searched) then ② will contact the source of that info (node edu.pl) to later find the answer.

5. If no info is in the cache then the server may forward the query (this depends on the configuration – forward

option must be turned on).

6. If — no information is found in
the cache
   — no forward or forward was
unsuccessful

then ② will access its hints
file. The hints file provides a list
of root name servers to query
in order to start the trip from
the top (root) to the host down
the DNS hierarchy.

The servers on different levels
are under controll of different
organisations. The organisations
may serve multiple domain
levels → so we have

distinction between zones and
domains.
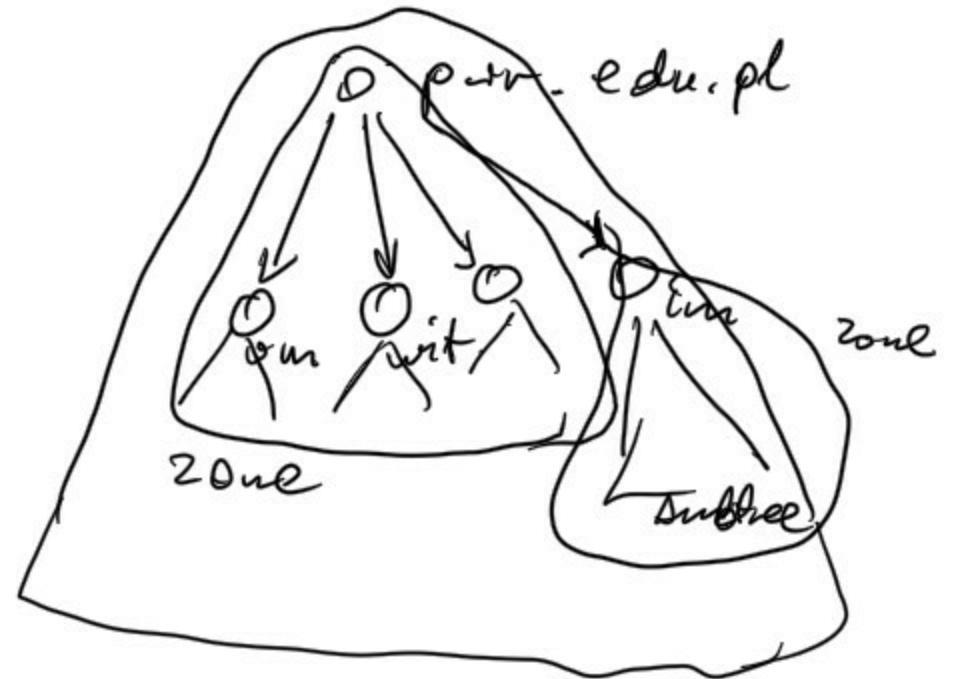
So admins of pwr.edu.pl zone
must configure records for
pwr... including subdomains
in the zone and must provide
delegation pointer to im.pwr.
edu.pl and to any child
zone.

This delegation in achieved by entering name server (NS) ressource record within the pwr.edu.pl zone. This record will reffer the resolver to the name server further down the tree.

The name server can be indicated also directly by IP address (A or AAAA records) — glue records

to glue NS host domain name to IP address of this host.

There should be two servers (for better robustness of the system). So the master and the slave / secondary servers are

~~and slavth~~ indicated.

The slaves obtain zone updates by the process called zone-transfer.

Each zone file has serial number.
↗
changes every time a change is applied to the zone.

— slave can check periodically

— or master may notify a slave (especially if the changes are frequent).

Transfer:

— entire zone configuration file can be transferred
  — absolute zone transfer (AXFR)
— incremental zone transfer (IXFR)