Kathará

kathara lab

dns

Version	2.0
Author(s)	L. Ariemma, G. Di Battista, M. Patrignani, M. Pizzonia, F. Ricci, M. Rimondini
E-mail	contact@kathara.org
Web	http://www.kathara.org/
Description	using the domain name system – kathara version of an existing netkit lab

copyright notice

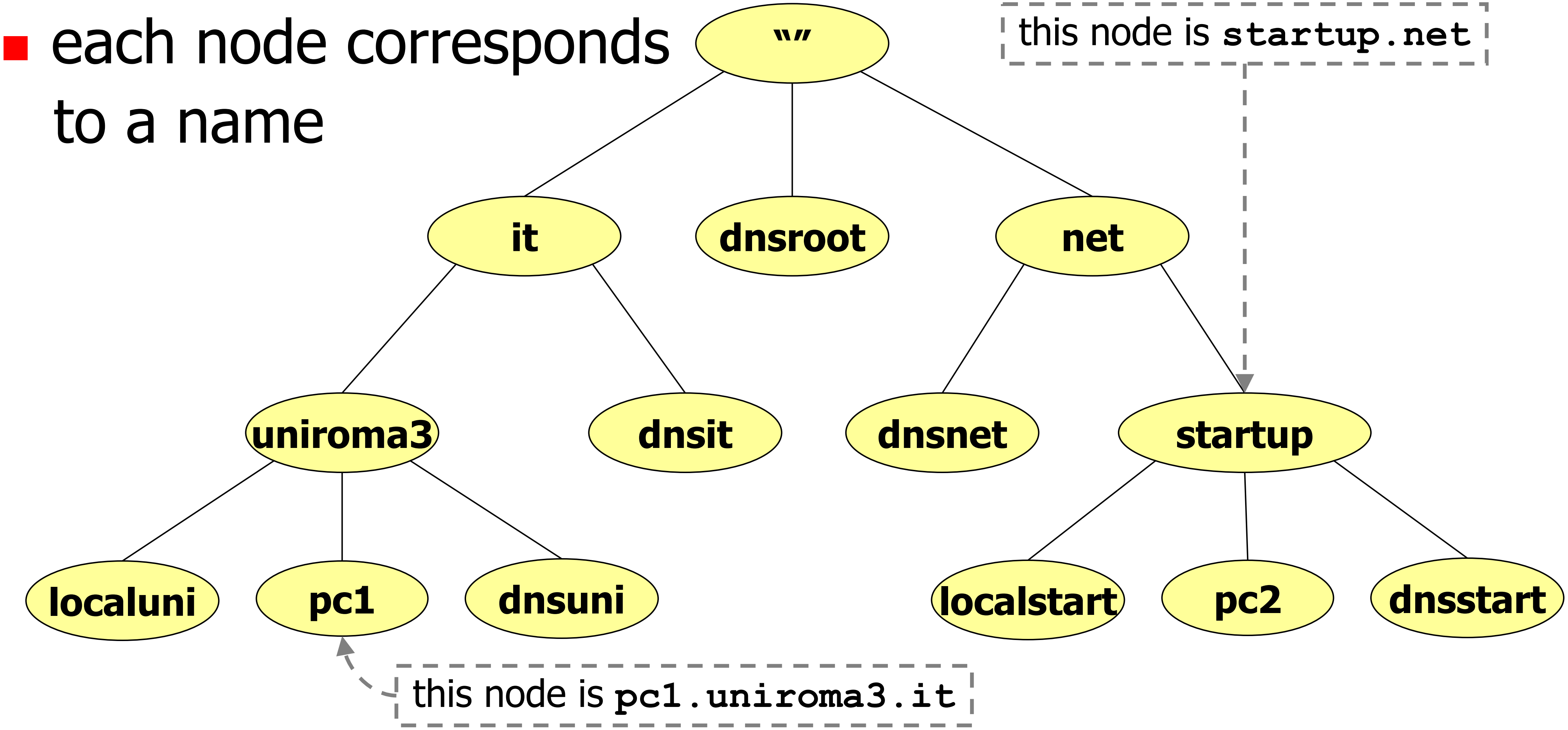
- All the pages/slides in this presentation, including but not limited to, images, photos, animations, videos, sounds, music, and text (hereby referred to as “material”) are protected by copyright.
- This material, with the exception of some multimedia elements licensed by other organizations, is property of the authors and/or organizations appearing in the first slide.
- This material, or its parts, can be reproduced and used for didactical purposes within universities and schools, provided that this happens for non-profit purposes.
- Information contained in this material cannot be used within network design projects or other products of any kind.
- Any other use is prohibited, unless explicitly authorized by the authors on the basis of an explicit agreement.
- The authors assume no responsibility about this material and provide this material “as is”, with no implicit or explicit warranty about the correctness and completeness of its contents, which may be subject to changes.
- This copyright notice must always be redistributed together with the material, or its portions.

about the dns

- takes care of associating names with ip addresses
- the name system is distributed over several nodes (hosts) that are hierarchically organized to form a tree
- each node in the hierarchy corresponds to a name
- a domain in the name system is a subtree
- a node in the hierarchy may be delegated to handle names for a particular zone
  - such a node is an authoritative server for that zone
- a zone is a domain which is devoid of those nodes having a different authoritative server (i.e., a tree without subtrees)

the dns name hierarchy

- each node corresponds to a name

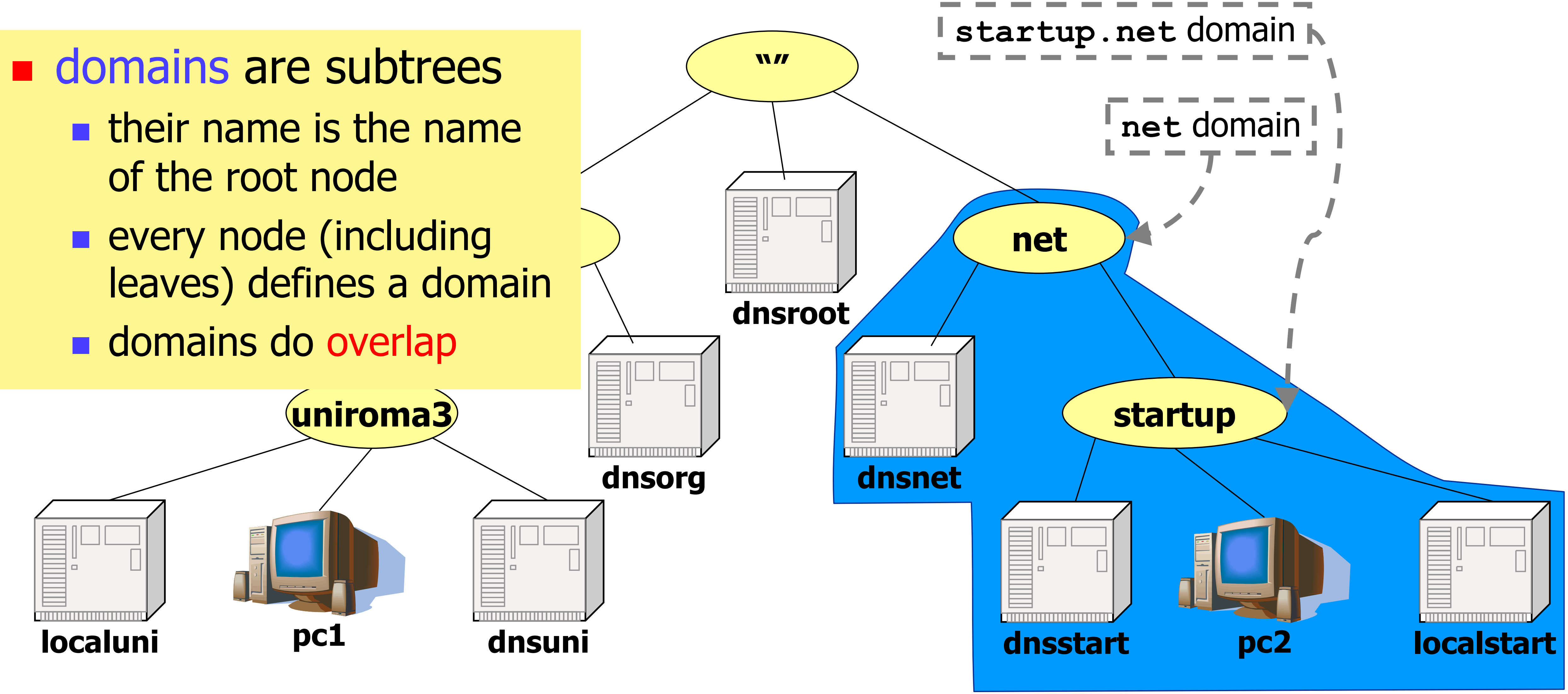


this node is `startup.net`

this node is `pc1.uniroma3.it`

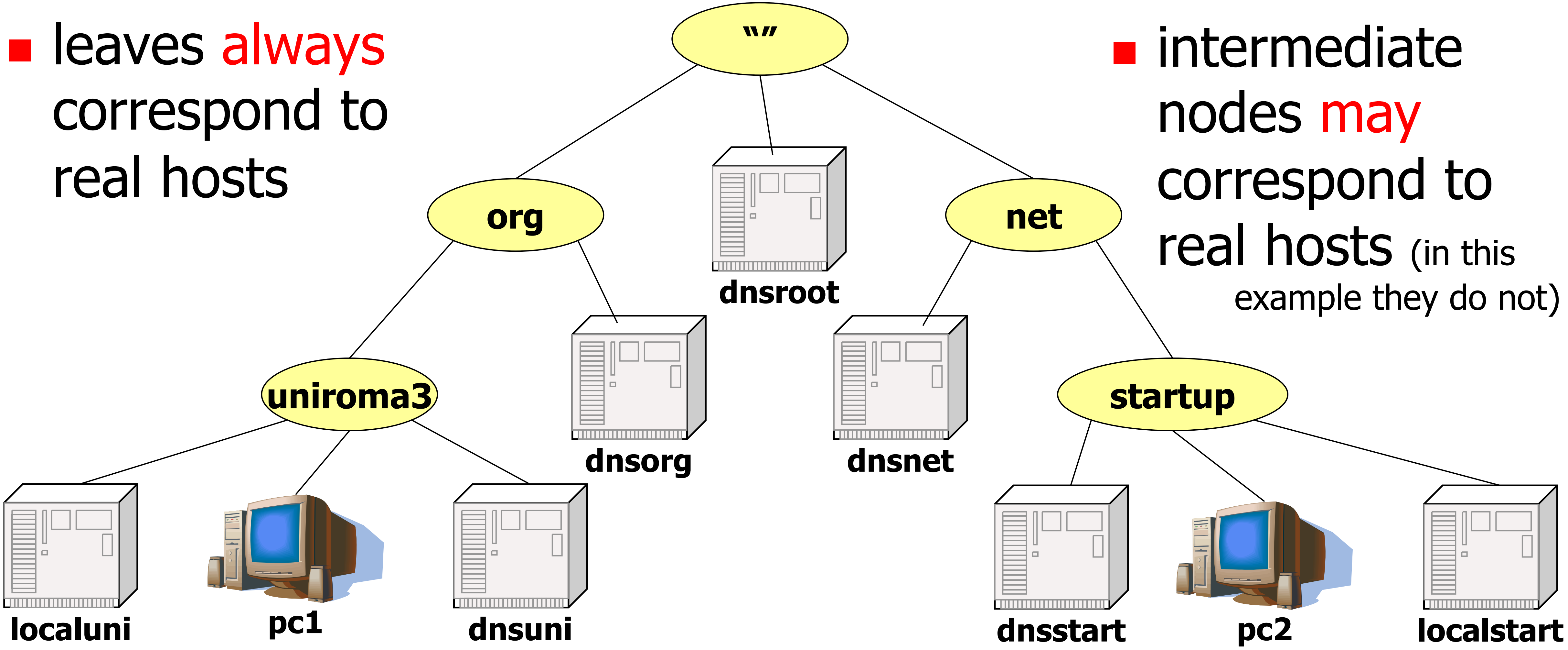
the dns name hierarchy

- domains are subtrees
  - their name is the name of the root node
  - every node (including leaves) defines a domain
  - domains do overlap



the dns name hierarchy

- leaves always correspond to real hosts

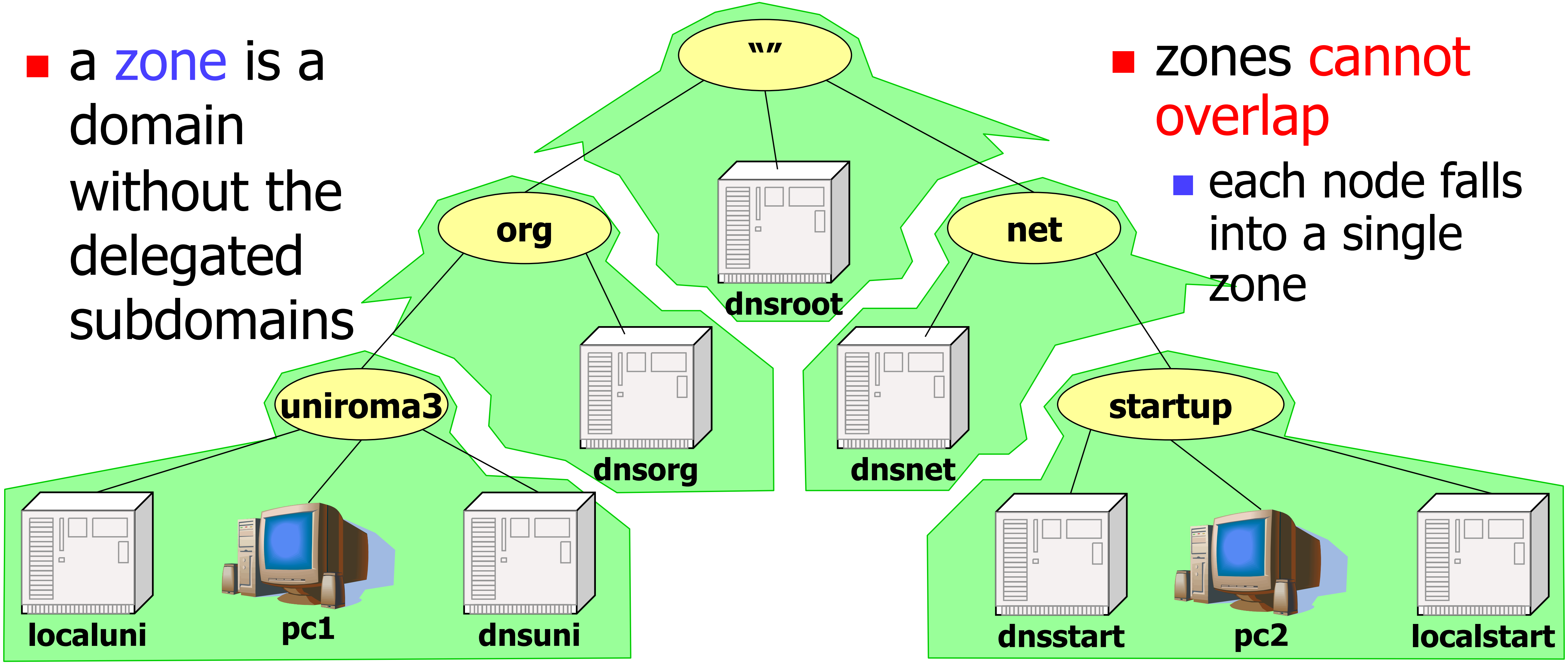


- intermediate nodes may correspond to real hosts (in this example they do not)

zones

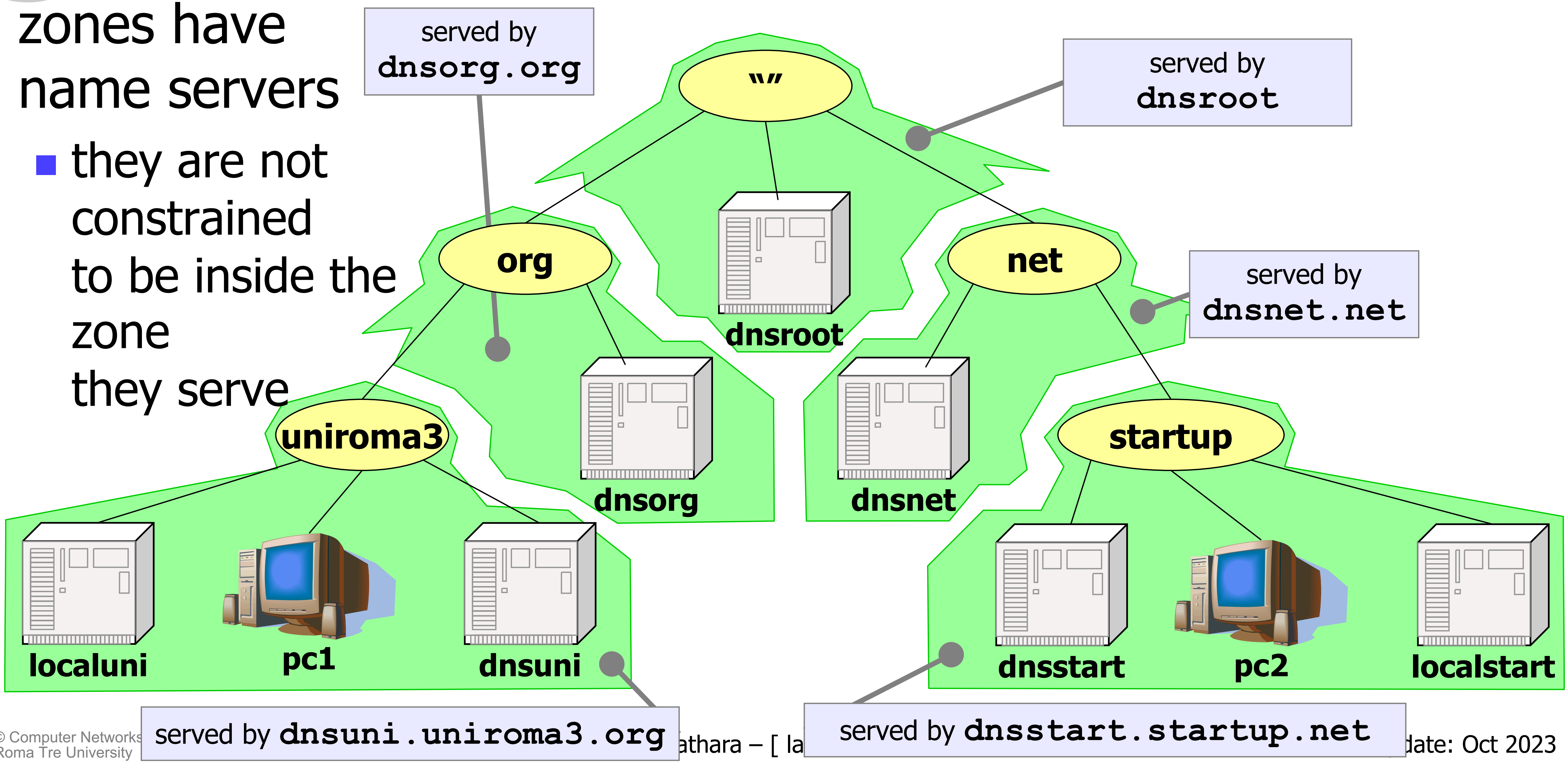
- a zone is a domain without the delegated subdomains

- zones cannot overlap
  - each node falls into a single zone



zones

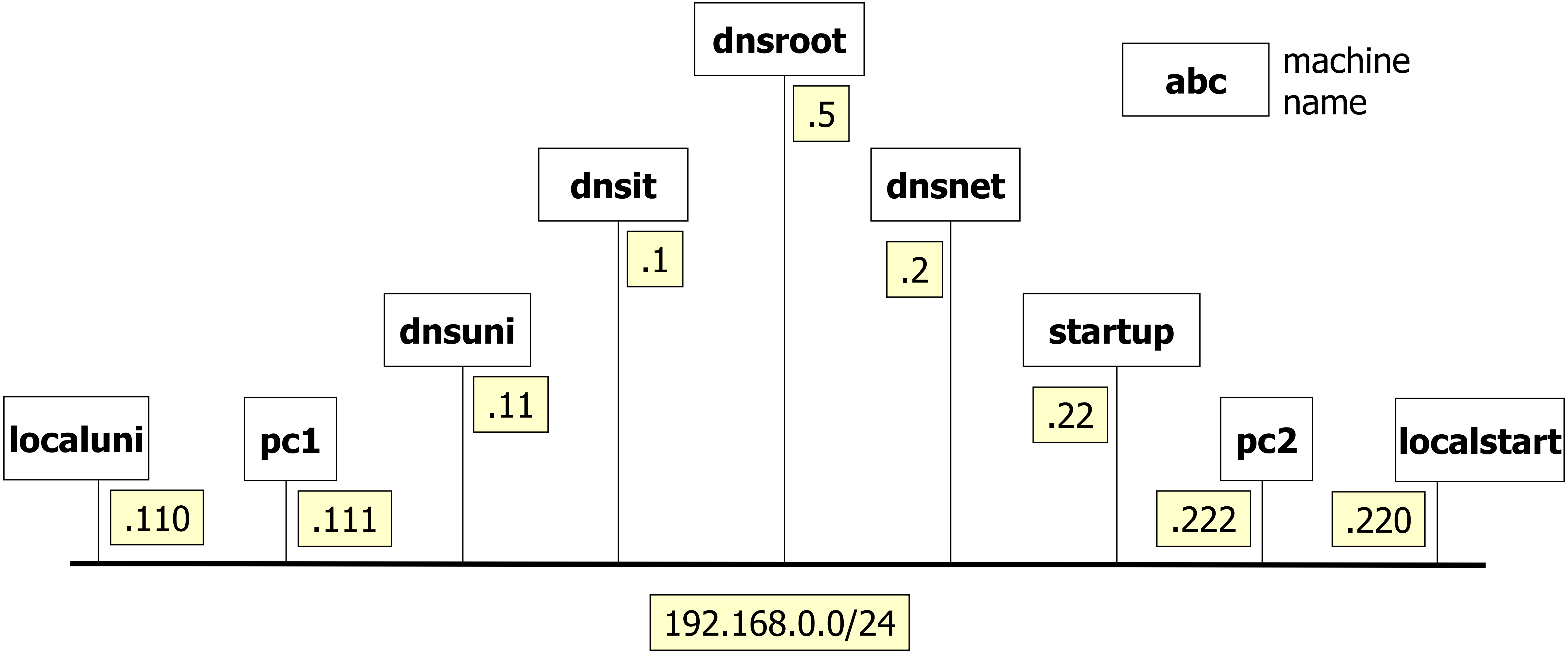
- zones have name servers
  - they are not constrained to be inside the zone they serve



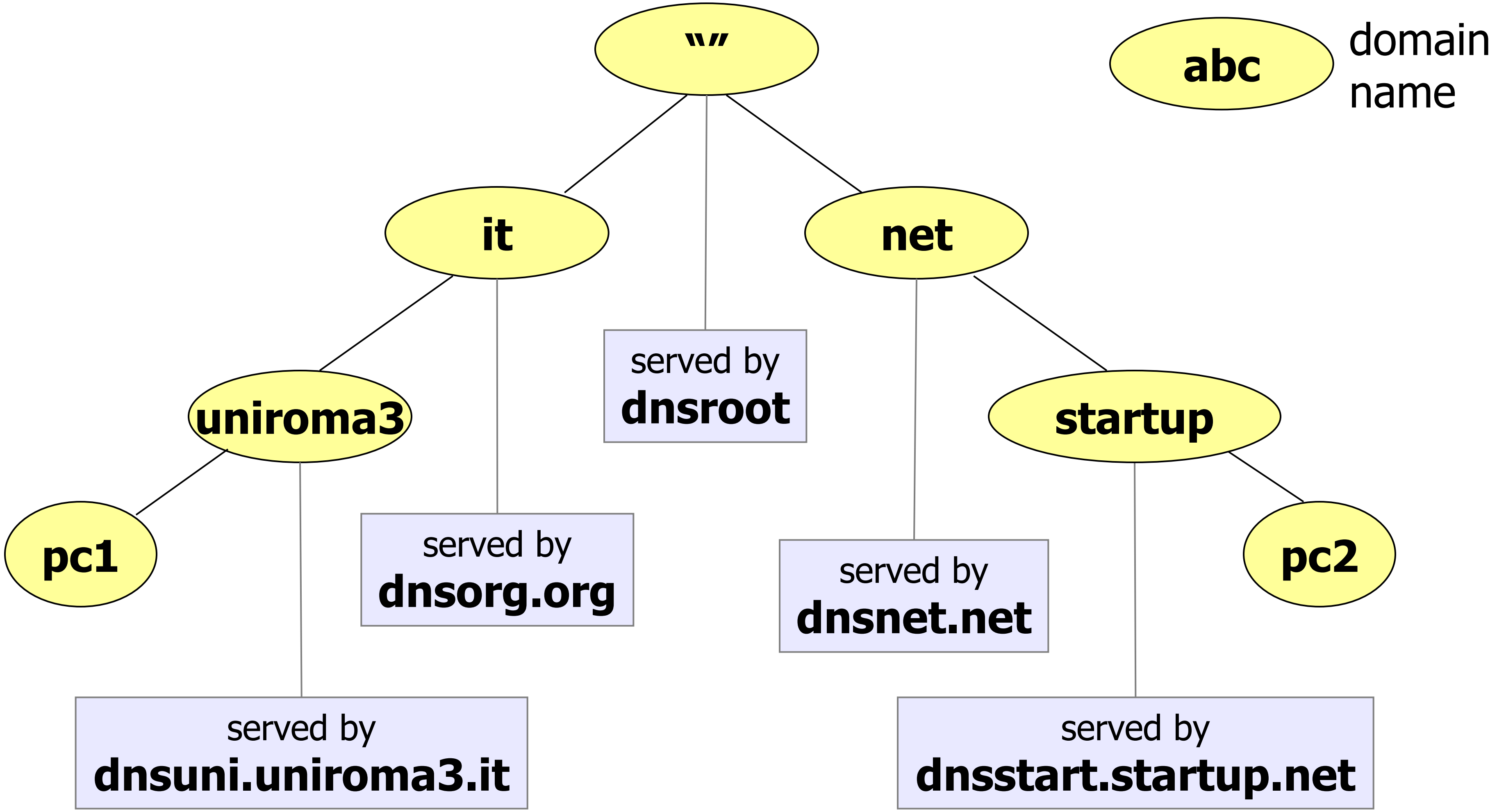
more about the dns

- the dns hierarchy is orthogonal with respect to the actual network topology
- in order to focus on the behavior of the dns we choose a flat topology, consisting of a single collision domain

step 1 – network topology



step 1 – dns (zone) hierarchy

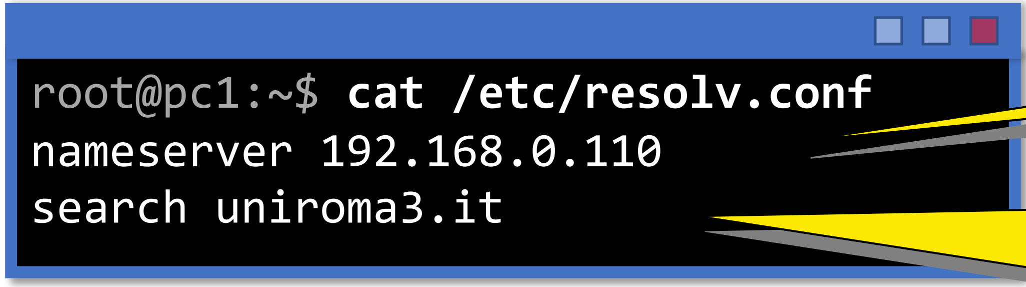


step 2 – starting the lab

- the lab is configured to
  - start all the 9 vms
  - automatically configure the network interfaces
  - automatically configure the authority name servers
  - automatically configure the local name servers
  - automatically start the name server software (bind) on each name server

step 2 – exploring the configuration

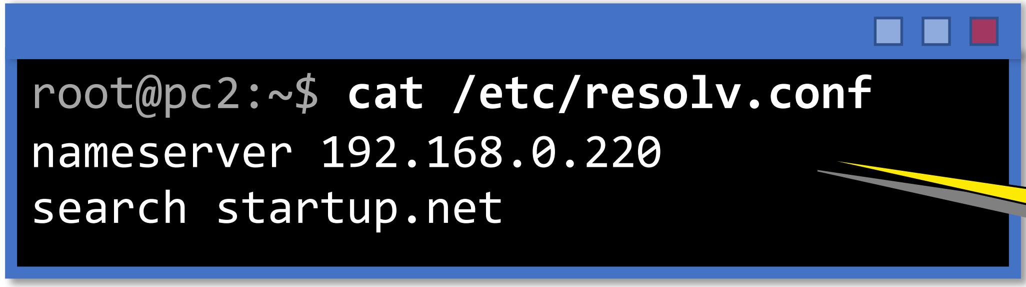
- configuration on the PCs consists of the specification of the default name server



```
root@pc1:~$ cat /etc/resolv.conf
nameserver 192.168.0.110
search uniroma3.it
```

`localuni.uniroma3.it`

suffix to append to unqualified names (e.g., asking to resolve **`dummy`** results in querying for **`dummy.uniroma3.it`**)



```
root@pc2:~$ cat /etc/resolv.conf
nameserver 192.168.0.220
search startup.net
```

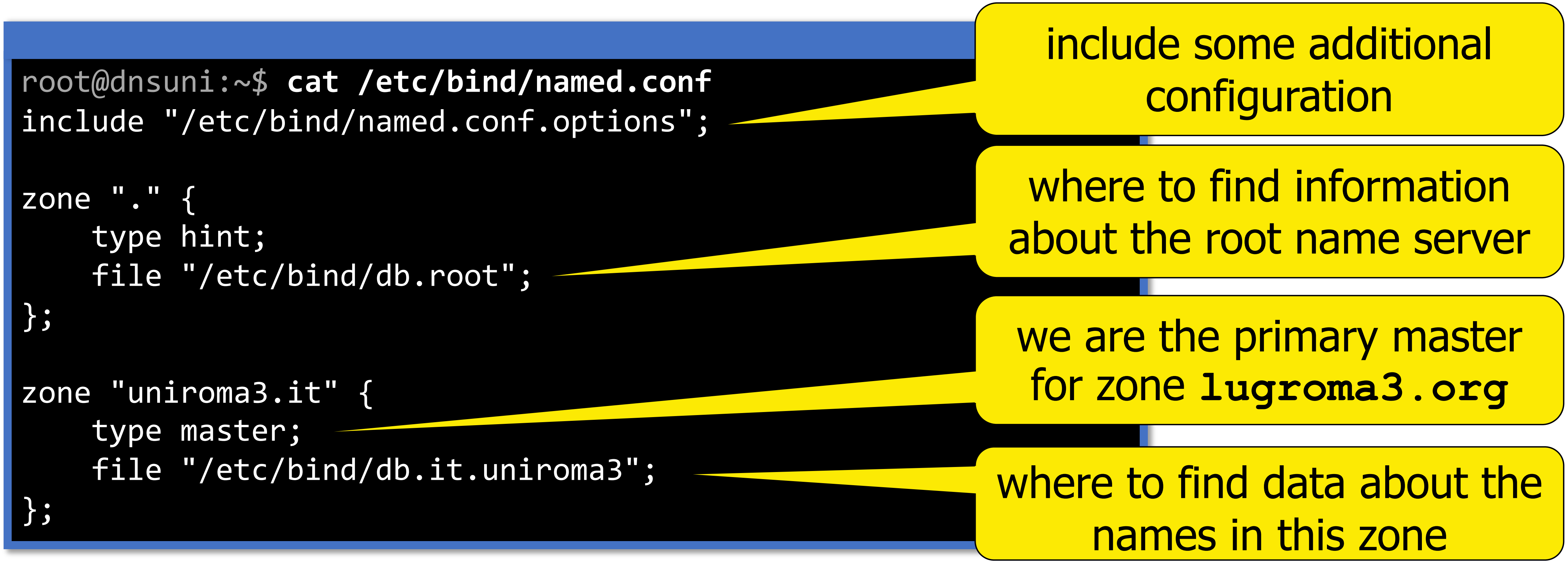
`localstart.startup.net`

step 2 – exploring the configuration

- configuration on the name servers specifies
  - associations between zones and name servers
  - information about the root name servers
  - authoritative information
  - associations between names and IP addresses
  - authorization to resolve recursive queries

step 2 – exploring the configuration

- configuration on the name servers specifies
  - associations between zones and name servers



```
root@dnsuni:~$ cat /etc/bind/named.conf
include "/etc/bind/named.conf.options";

zone "." {
    type hint;
    file "/etc/bind/db.root";
};

zone "uniroma3.it" {
    type master;
    file "/etc/bind/db.it.uniroma3";
};
```

include some additional configuration

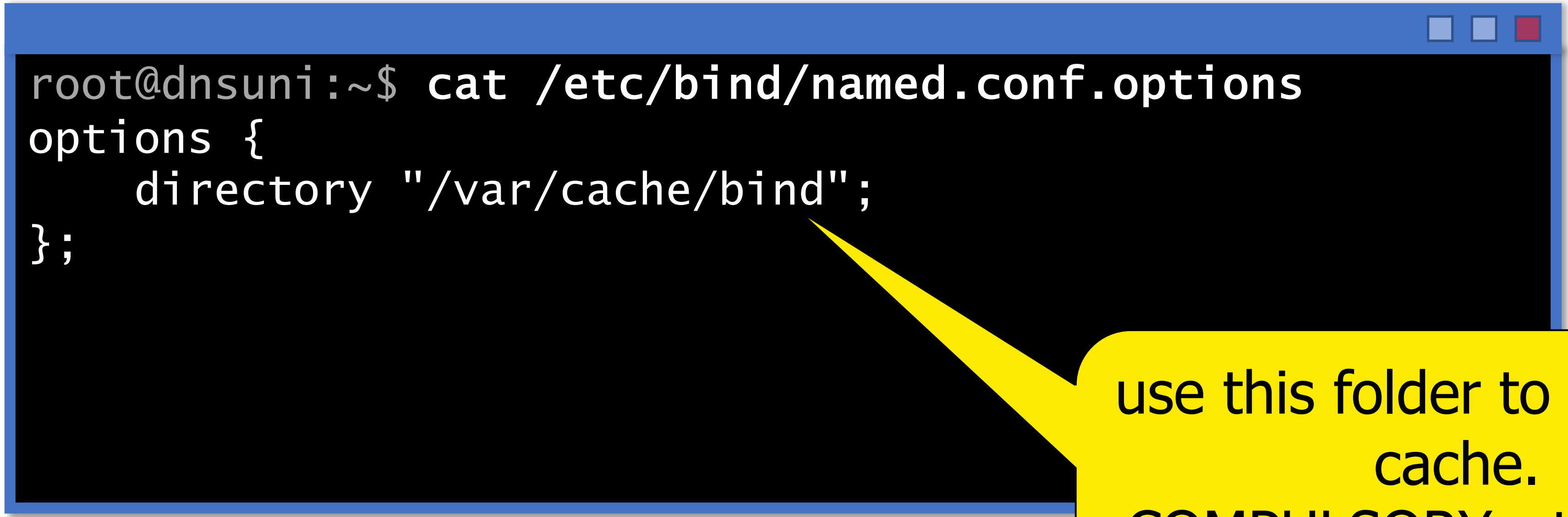
where to find information about the root name server

we are the primary master for zone `lugroma3.org`

where to find data about the names in this zone

step 2 – exploring the configuration

- configuration on the name servers specifies
  - additional configuration



```
root@dnsuni:~$ cat /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
};
```

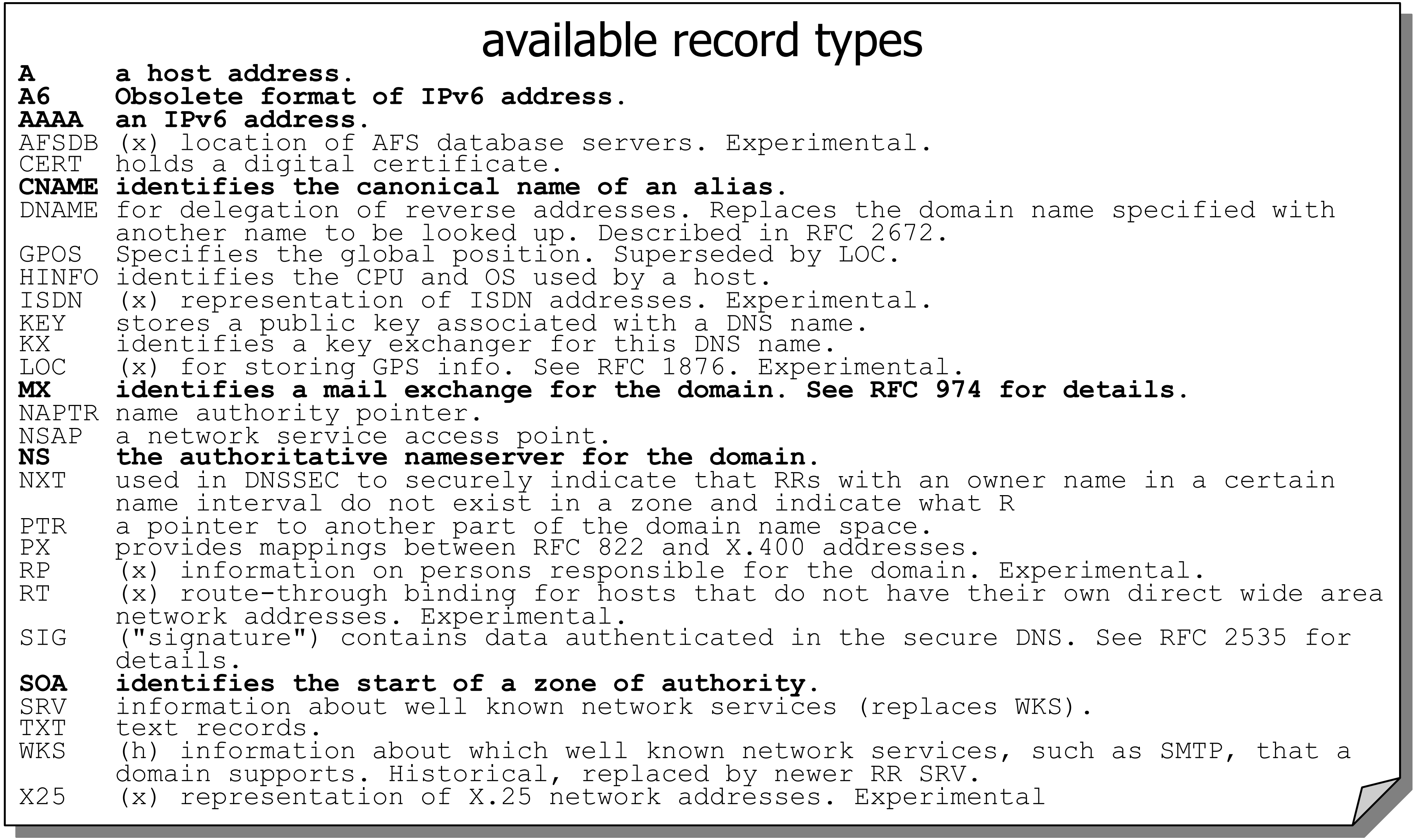
use this folder to store the cache. COMPULSORY, otherwise, named wont ‘t start

format of a resource record

```
<domain> <class> <type> <rdata>
```

- domain: the record owner (=domain to which the record refers)
- class: usually IN (=Internet system); may be HS (=hesiod) or CH (=chaos)
- type: see next slide...
- rdata: record data (depends on the record type)

step 2 – exploring the configuration

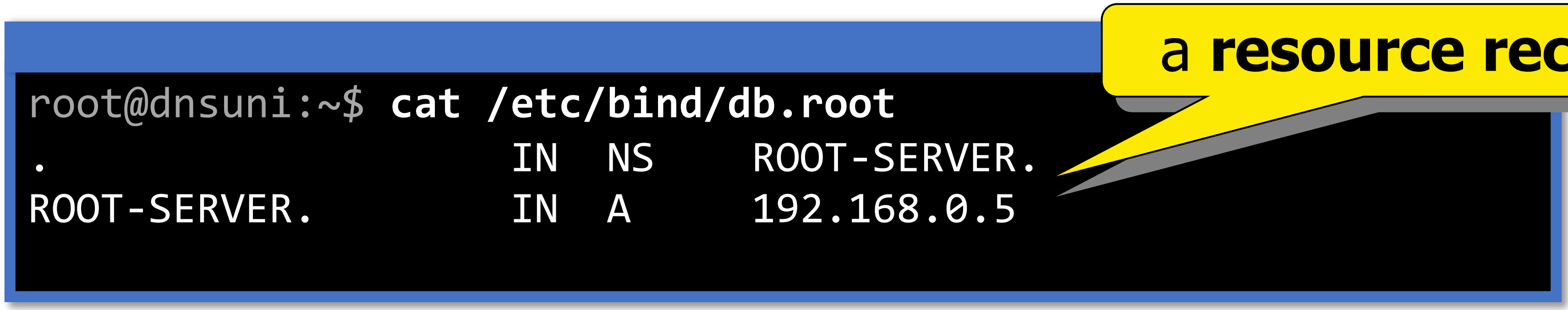


available record types

```
A      a host address.
A6     Obsolete format of IPv6 address.
AAAA   an IPv6 address.
AFSDB  (x) location of AFS database servers. Experimental.
CERT   holds a digital certificate.
CNAME  identifies the canonical name of an alias.
DNAME  for delegation of reverse addresses. Replaces the domain name specified with
       another name to be looked up. Described in RFC 2672.
GPOS   Specifies the global position. Superseded by LOC.
HINFO  identifies the CPU and OS used by a host.
ISDN   (x) representation of ISDN addresses. Experimental.
KEY    stores a public key associated with a DNS name.
KX     identifies a key exchanger for this DNS name.
LOC    (x) for storing GPS info. See RFC 1876. Experimental.
MX     identifies a mail exchange for the domain. See RFC 974 for details.
NAPTR  name authority pointer.
NSAP   a network service access point.
NS     the authoritative nameserver for the domain.
NXT    used in DNSSEC to securely indicate that RRs with an owner name in a certain
       name interval do not exist in a zone and indicate what R
PTR    a pointer to another part of the domain name space.
PX     provides mappings between RFC 822 and X.400 addresses.
RP     (x) information on persons responsible for the domain. Experimental.
RT     (x) route-through binding for hosts that do not have their own direct wide area
       network addresses. Experimental.
SIG    ("signature") contains data authenticated in the secure DNS. See RFC 2535 for
       details.
SOA    identifies the start of a zone of authority.
SRV    information about well known network services (replaces WKS).
TXT    text records.
WKS    (h) information about which well known network services, such as SMTP, that a
       domain supports. Historical, replaced by newer RR SRV.
X25    (x) representation of X.25 network addresses. Experimental
```

step 2 – exploring the configuration

- configuration on the name servers specifies
  - information about the root name servers

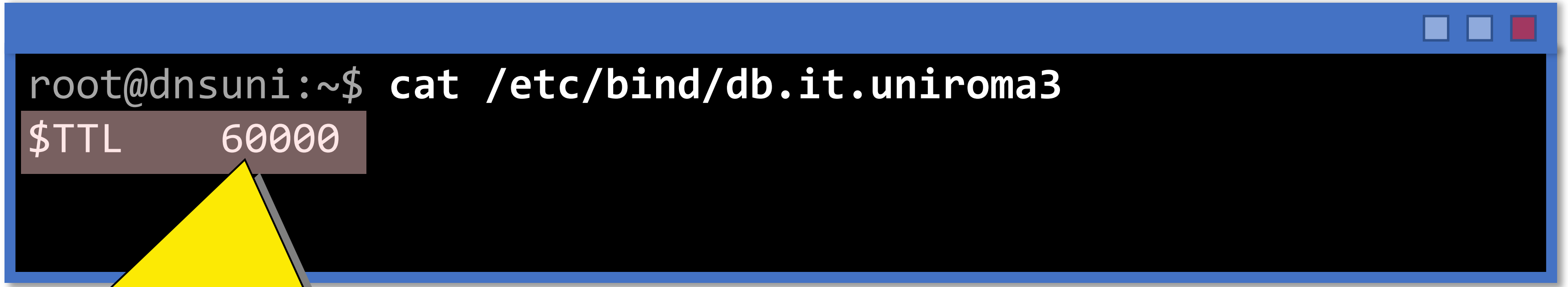


```
root@dnsuni:~$ cat /etc/bind/db.root
.                   IN  NS    ROOT-SERVER.
ROOT-SERVER.        IN  A     192.168.0.5
```

a **resource record**

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

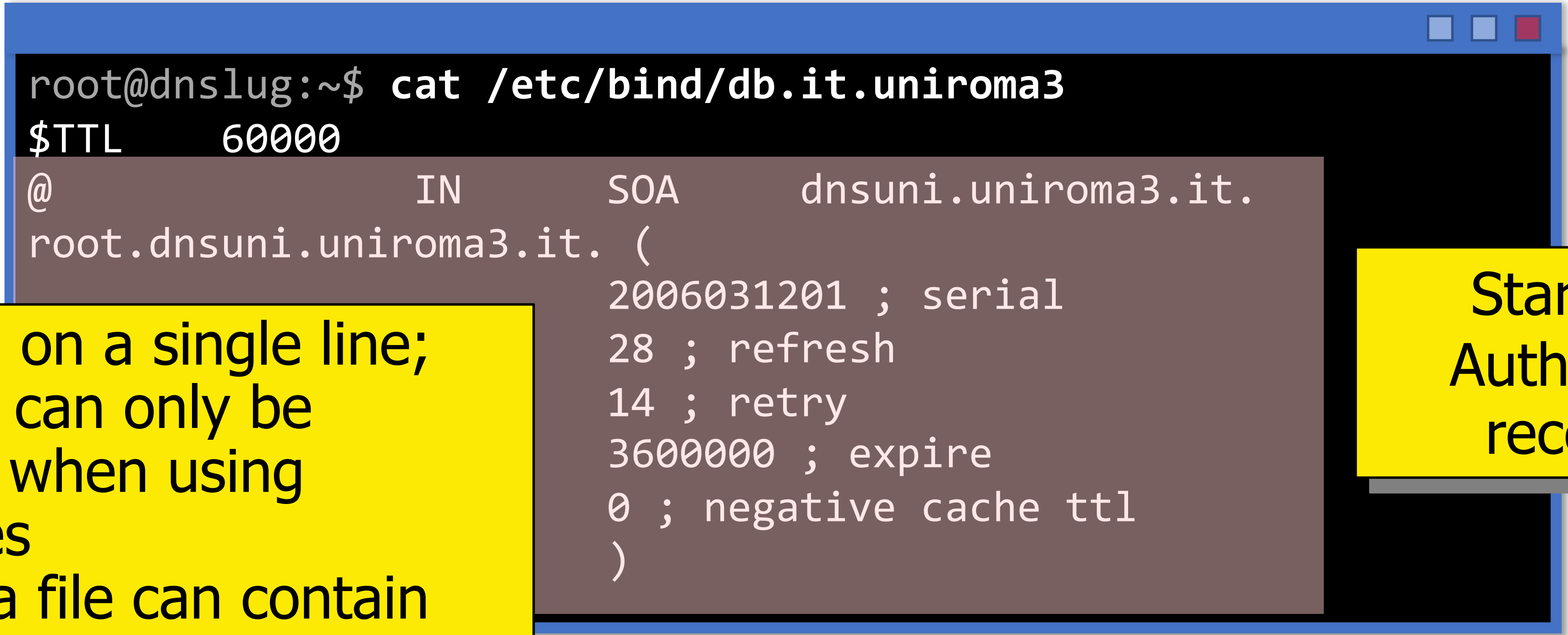


```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL     60000
```

time to live, in seconds
(determines how long a resource
record should be cached)

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



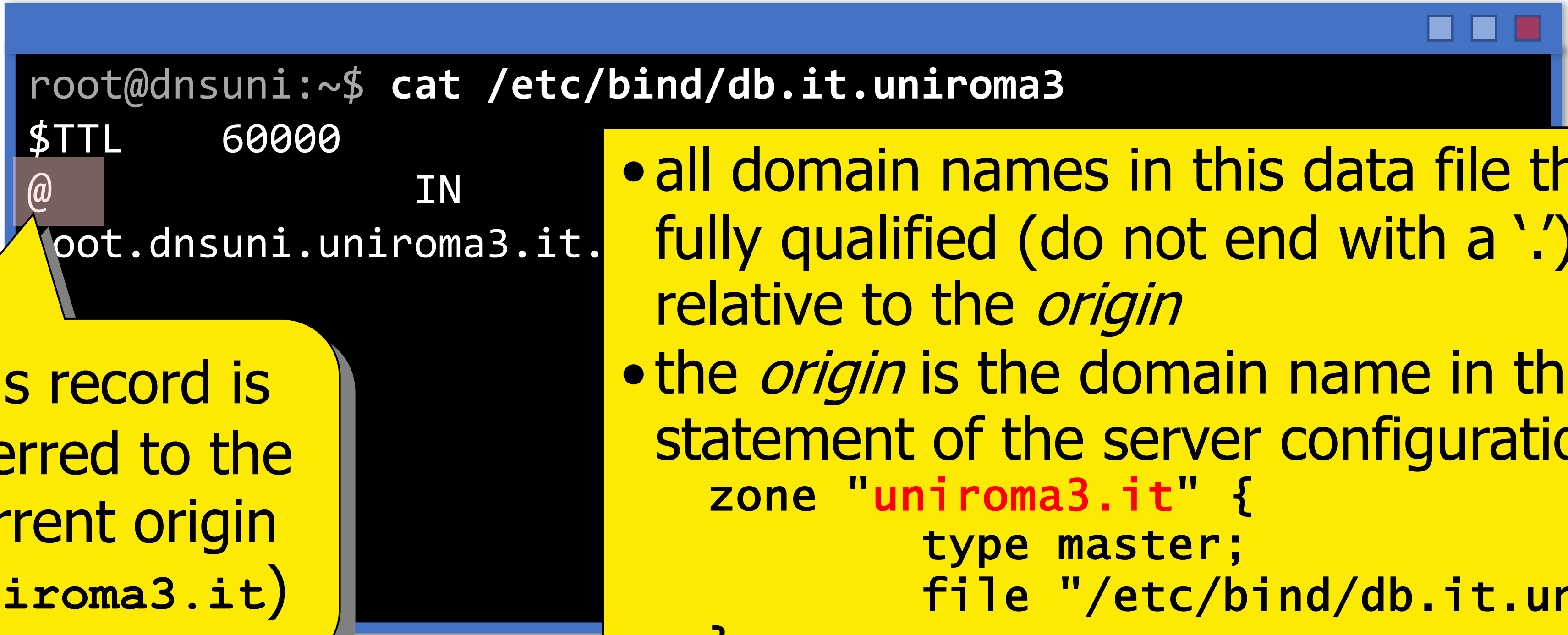
```
root@dnslug:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                        2006031201 ; serial
                        28 ; refresh
                        14 ; retry
                        3600000 ; expire
                        0 ; negative cache ttl
                        )
```

Start of Authority record

- must be all on a single line; line breaks can only be introduced when using parentheses
- a zone data file can contain only one SOA record

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@                   IN
 oot.dnsuni.uniroma3.it.
```

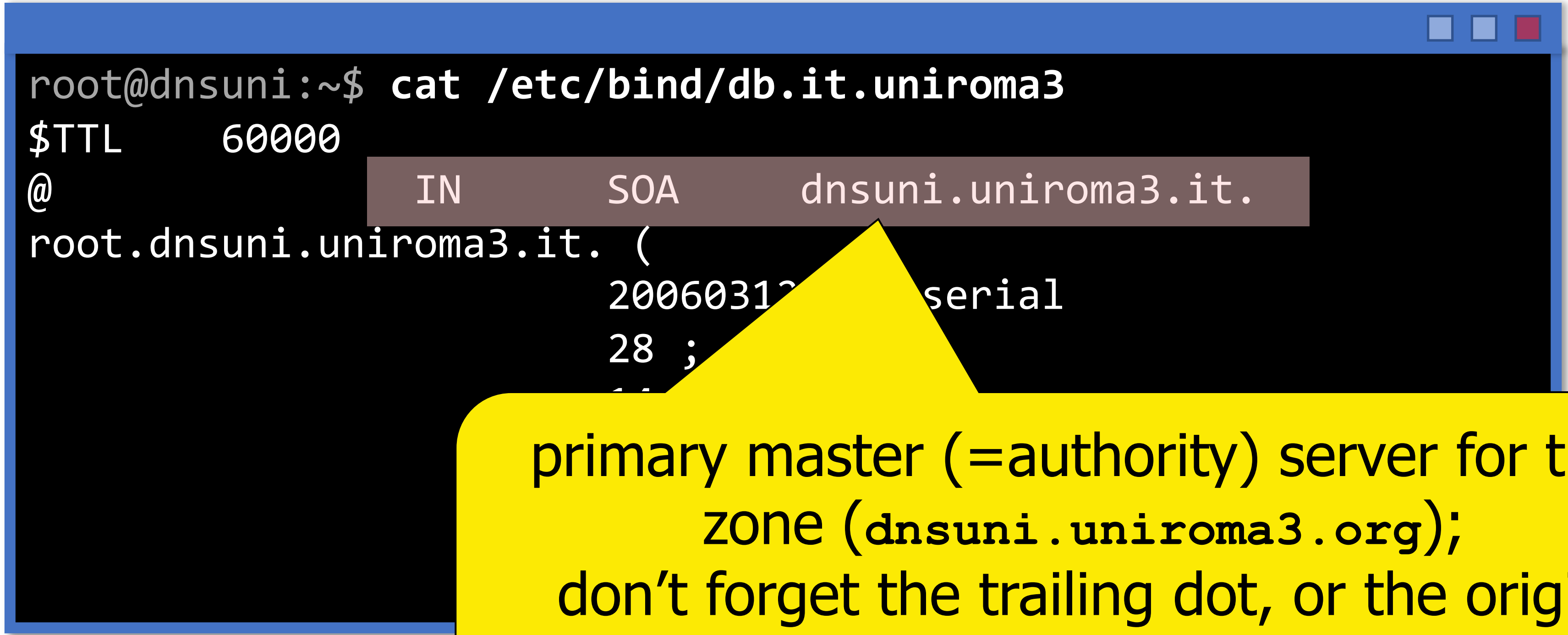
this record is referred to the current origin (`uniroma3.it`)

- all domain names in this data file that are not fully qualified (do not end with a '.') are relative to the *origin*
- the *origin* is the domain name in the *zone* statement of the server configuration file:

```
  zone "uniroma3.it" {
          type master;
          file "/etc/bind/db.it.uniroma3";
  };
```

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

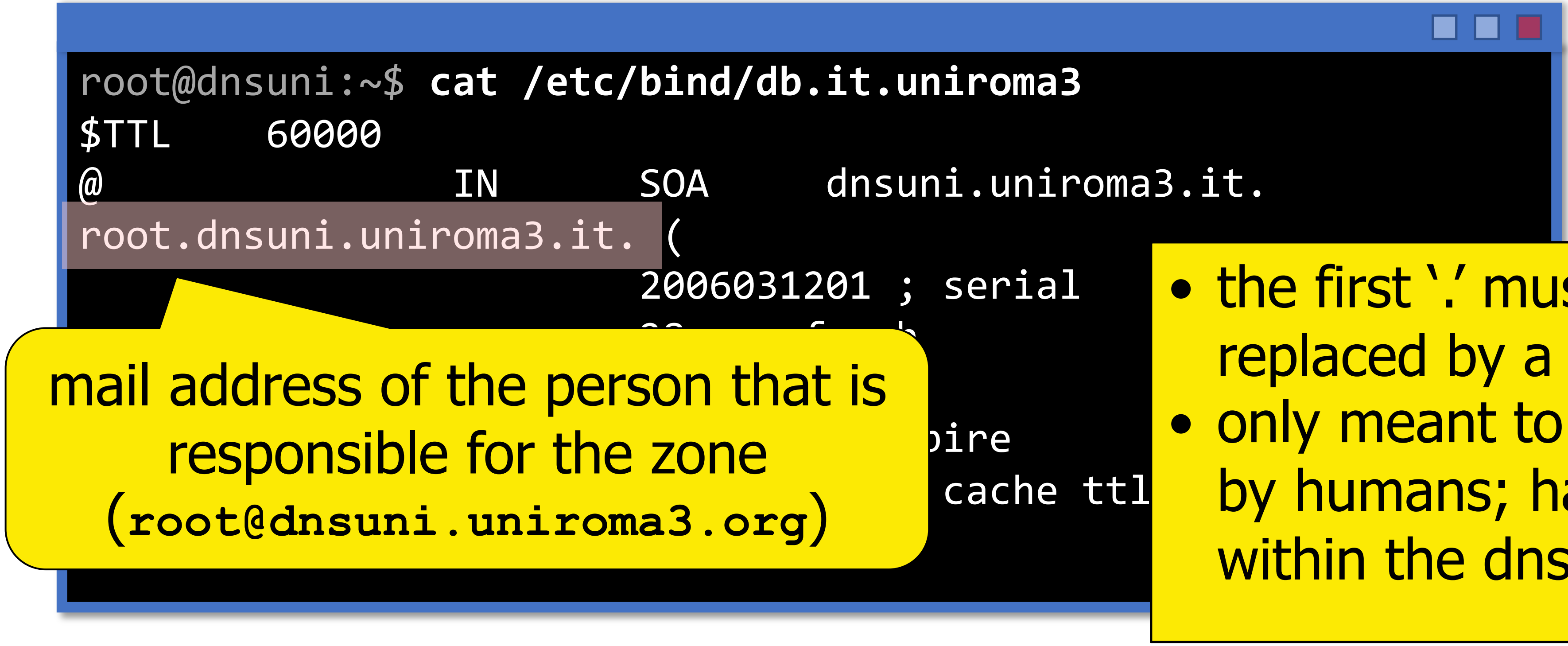


```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@              IN         SOA        dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                                2006031       serial
                                28 ;
```

primary master (=authority) server for this zone (**dnsuni.uniroma3.org**); don’t forget the trailing dot, or the origin name (**uniroma3.org**) would be appended!

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



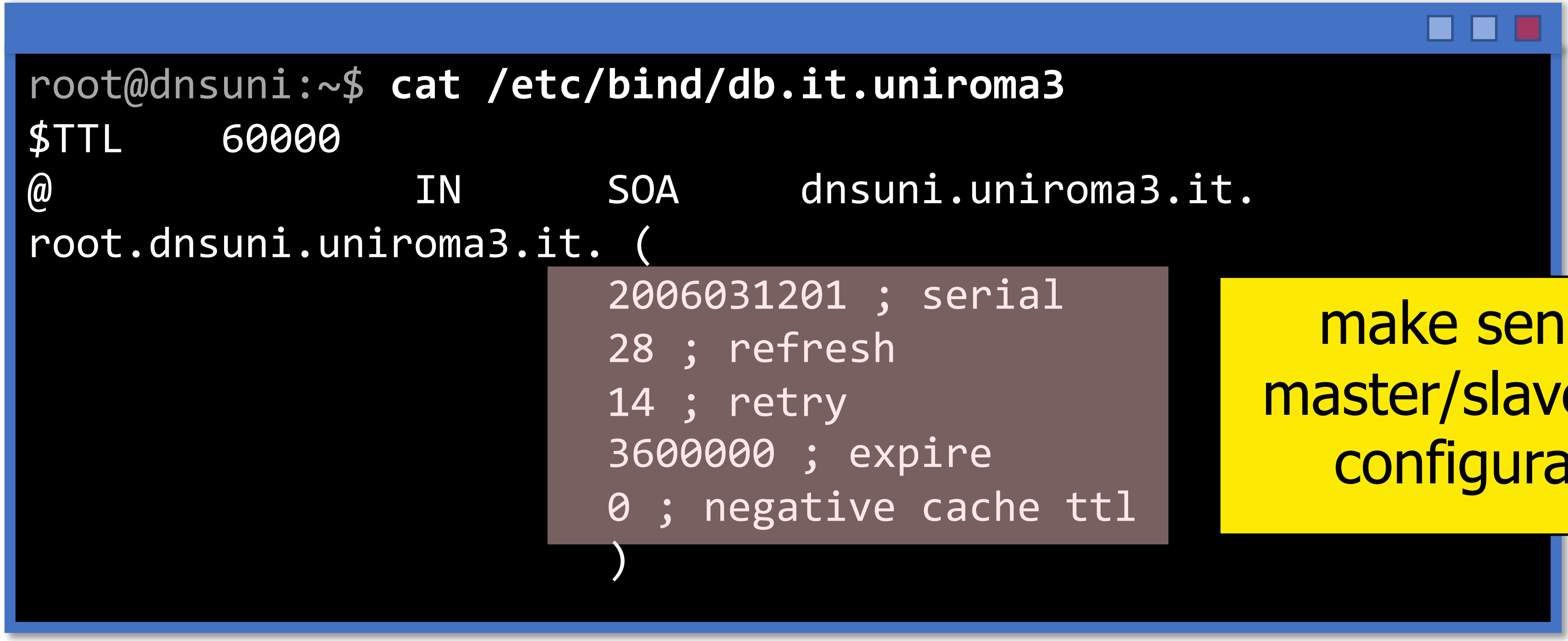
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                        2006031201 ; serial
                                pire
                                cache ttl
```

mail address of the person that is responsible for the zone (**root@dnsuni.uniroma3.org**)

- the first '.' must be replaced by a '@'
- only meant to be used by humans; has no use within the dns service

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

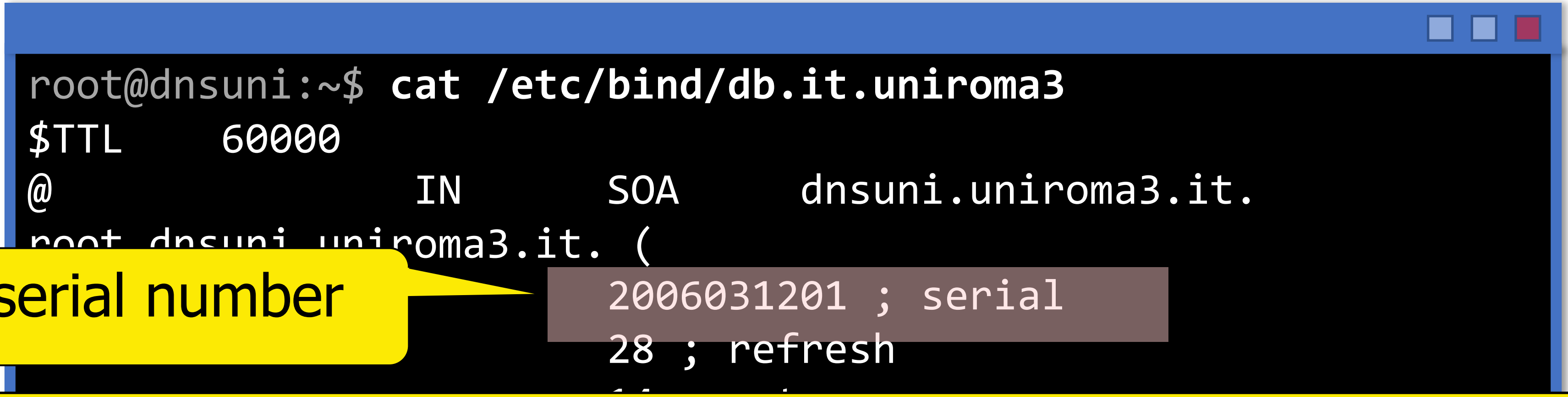


```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                        2006031201 ; serial
                        28 ; refresh
                        14 ; retry
                        3600000 ; expire
                        0 ; negative cache ttl
                        )
```

make sense for master/slave server configurations

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



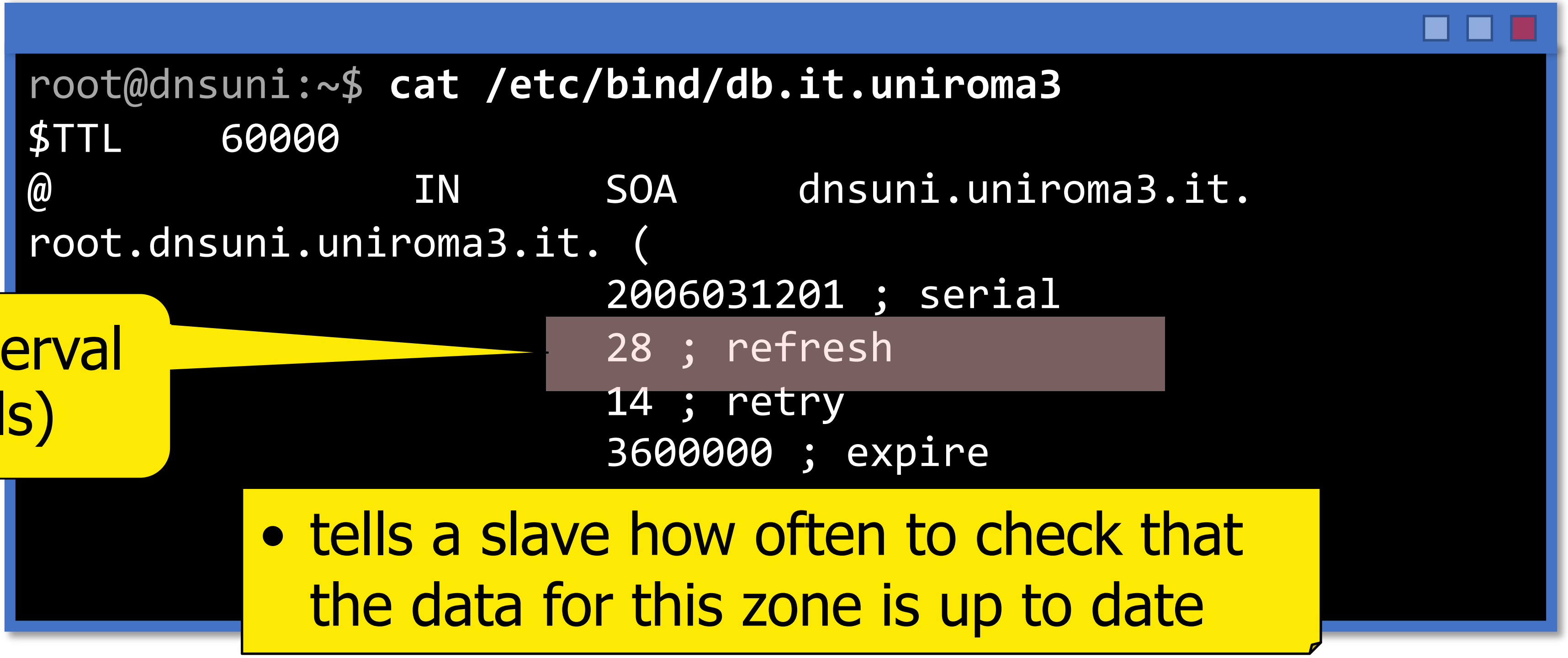
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@                   IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                            2006031201 ; serial
                            28 ; refresh
```

serial number

- determines how recent the information is
- influences all data within the zone
- conventional format:
  YYYYMMDDNN (year, month, day, # of changes within that day)

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



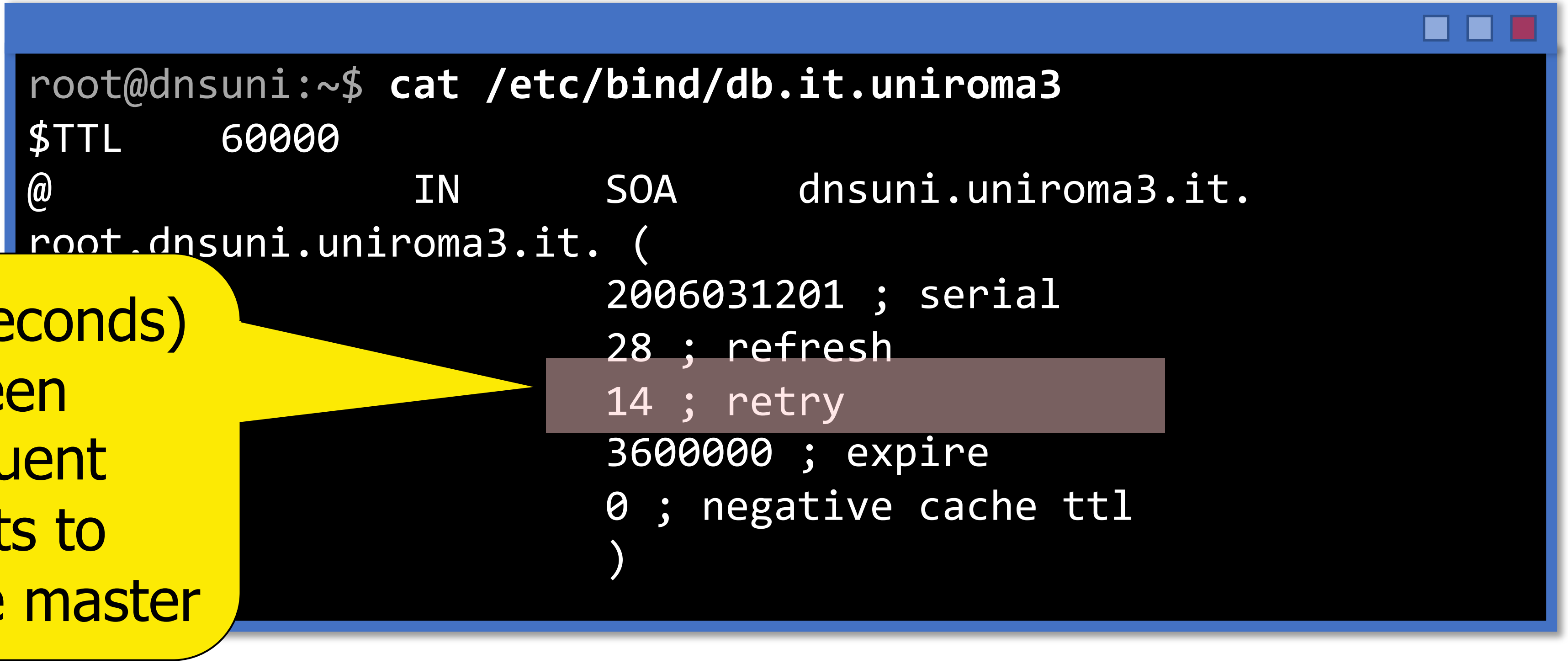
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@                IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                         2006031201 ; serial
                         28 ; refresh
                         14 ; retry
                         3600000 ; expire
```

refresh interval (seconds)

- tells a slave how often to check that the data for this zone is up to date

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

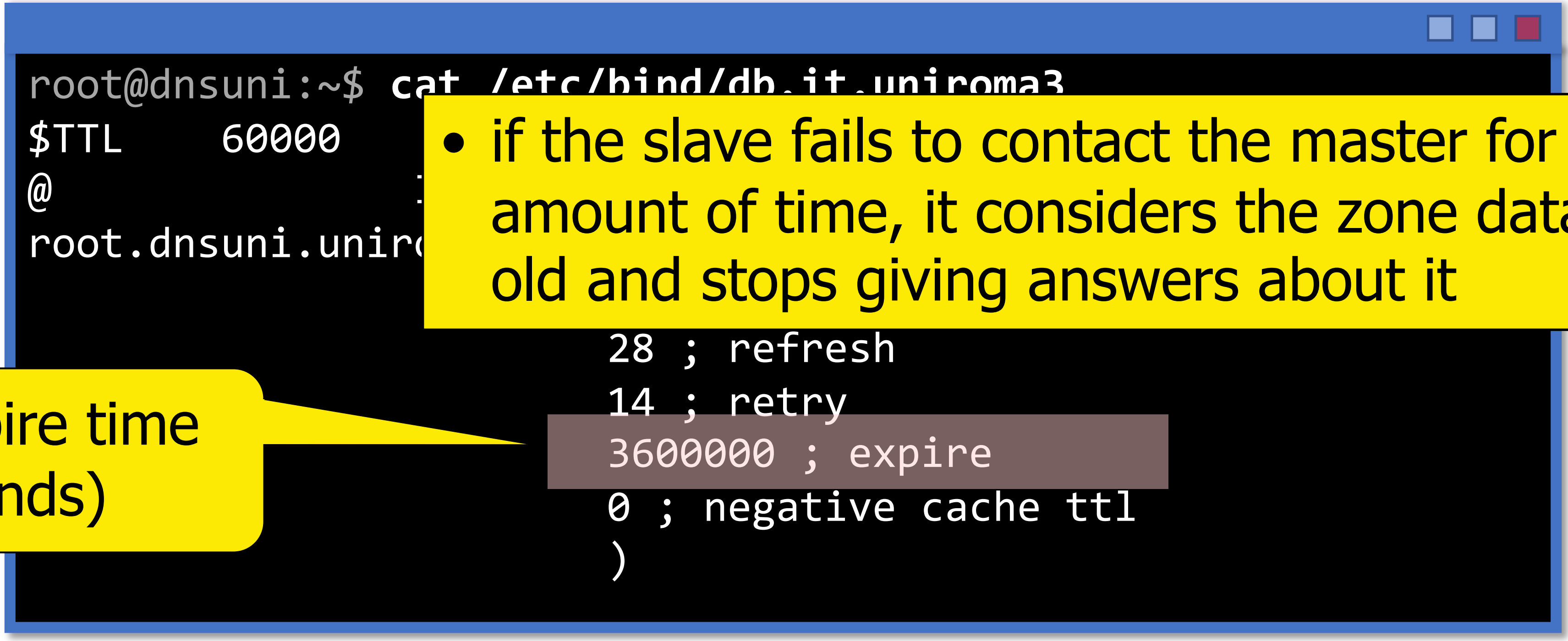


```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@                IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                         2006031201 ; serial
                         28 ; refresh
                         14 ; retry
                         3600000 ; expire
                         0 ; negative cache ttl
                         )
```

interval (seconds) between subsequent attempts to contact the master

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information



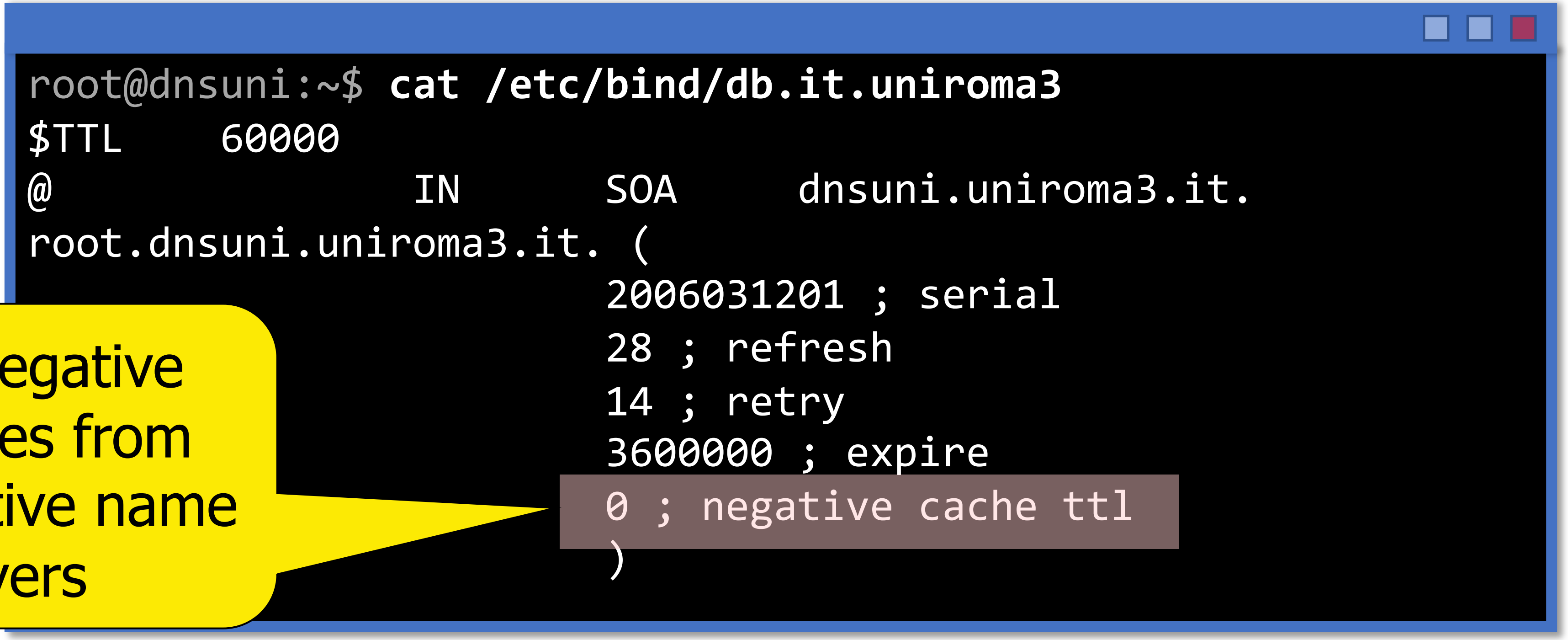
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@
root.dnsuni.unir

                28 ; refresh
                14 ; retry
                3600000 ; expire
                0 ; negative cache ttl
                )
```

- if the slave fails to contact the master for this amount of time, it considers the zone data too old and stops giving answers about it

slave expire time (seconds)

step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

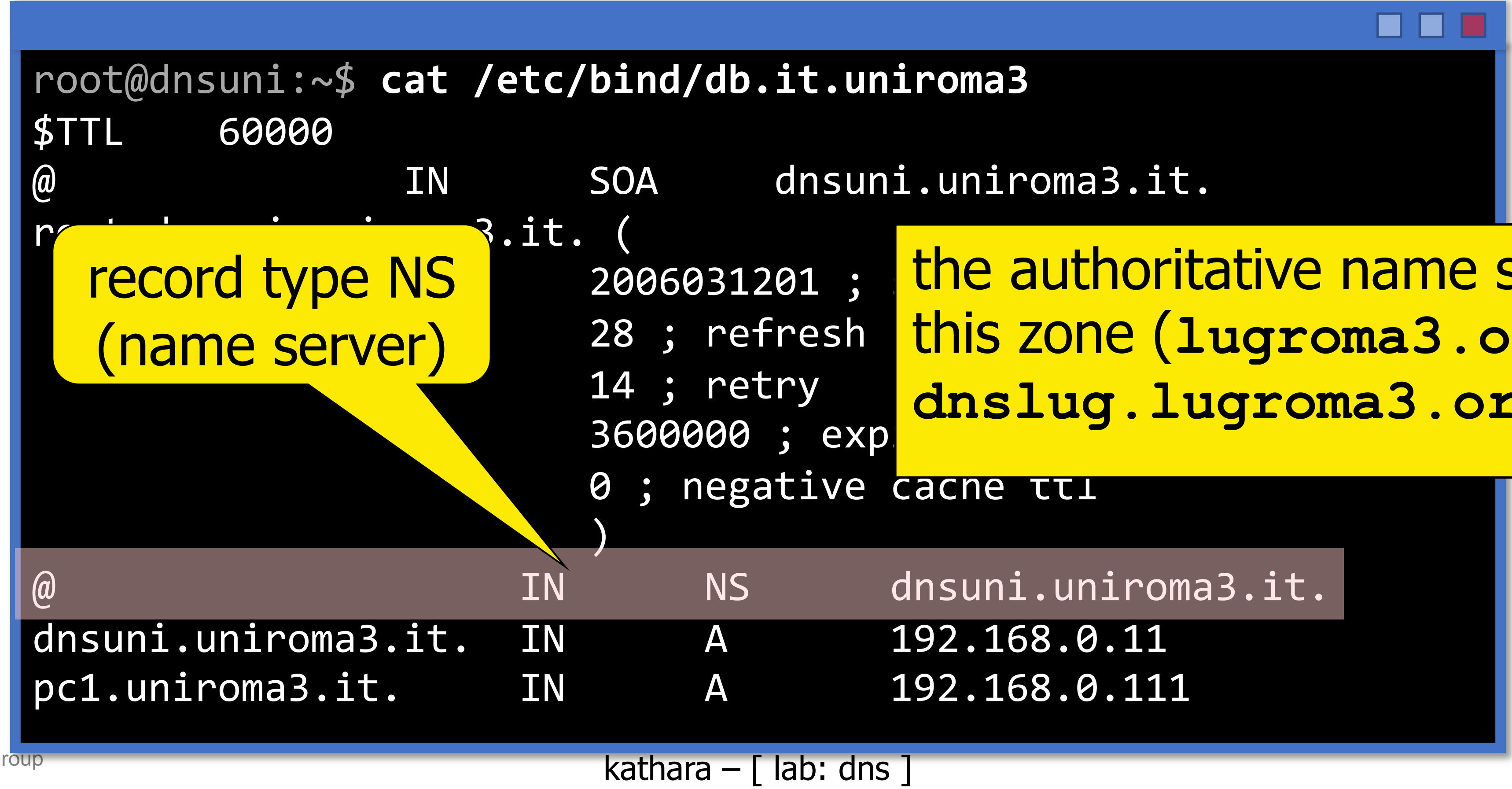


```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                        2006031201 ; serial
                        28 ; refresh
                        14 ; retry
                        3600000 ; expire
                        0 ; negative cache ttl
                        )
```

ttl for negative responses from authoritative name servers

step 2 – exploring the configuration

- configuration on the name servers specifies
  - associations between names and ip addresses



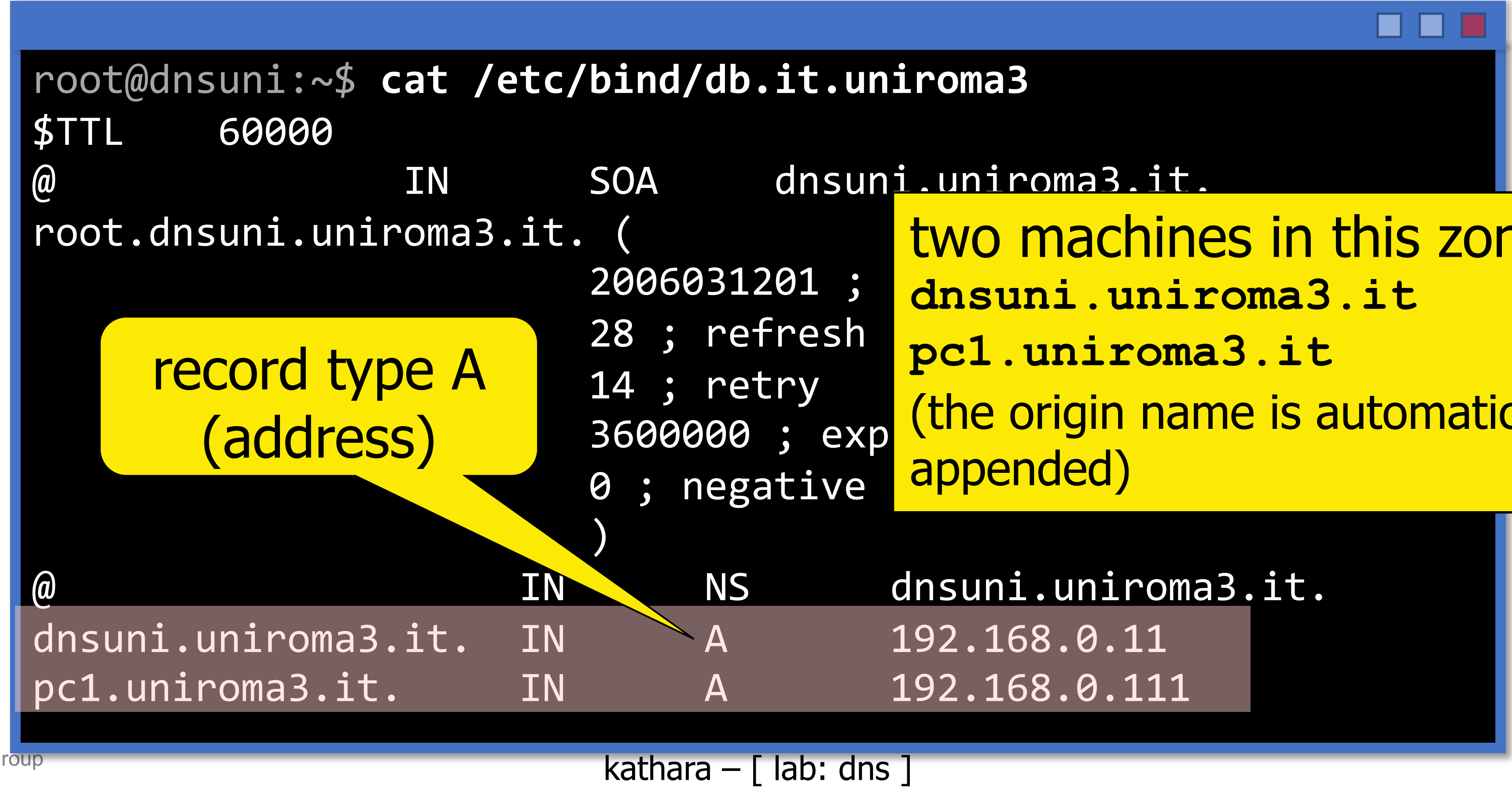
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
r                 3.it. (
                        2006031201 ;
                        28 ; refresh
                        14 ; retry
                        3600000 ; exp
                        0 ; negative cache ttl
                        )
@                   IN      NS      dnsuni.uniroma3.it.
dnsuni.uniroma3.it. IN      A       192.168.0.11
pc1.uniroma3.it.    IN      A       192.168.0.111
```

record type NS (name server)

the authoritative name server for this zone (**`lugroma3.org`**) is **`dnslug.lugroma3.org`**

step 2 – exploring the configuration

- configuration on the name servers specifies
  - associations between names and ip addresses



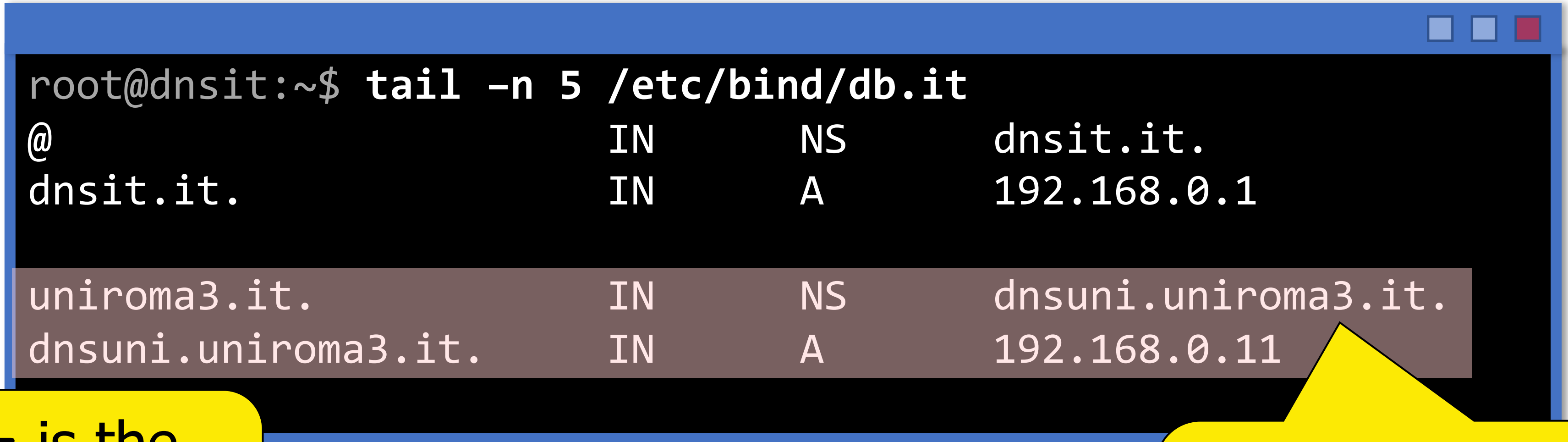
```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@               IN      SOA     dnsuni.uniroma3.it.
root.dnsuni.uniroma3.it. (
                        2006031201 ;
                        28 ; refresh
                        14 ; retry
                        3600000 ; exp
                        0 ; negative
                        )
@                    IN      NS      dnsuni.uniroma3.it.
dnsuni.uniroma3.it.  IN      A       192.168.0.11
pc1.uniroma3.it.     IN      A       192.168.0.111
```

record type A (address)

two machines in this zone:
dnsuni.uniroma3.it
pc1.uniroma3.it
(the origin name is automatically appended)

step 2 – exploring the configuration

- configuration on the name servers specifies
  - associations between names and ip addresses



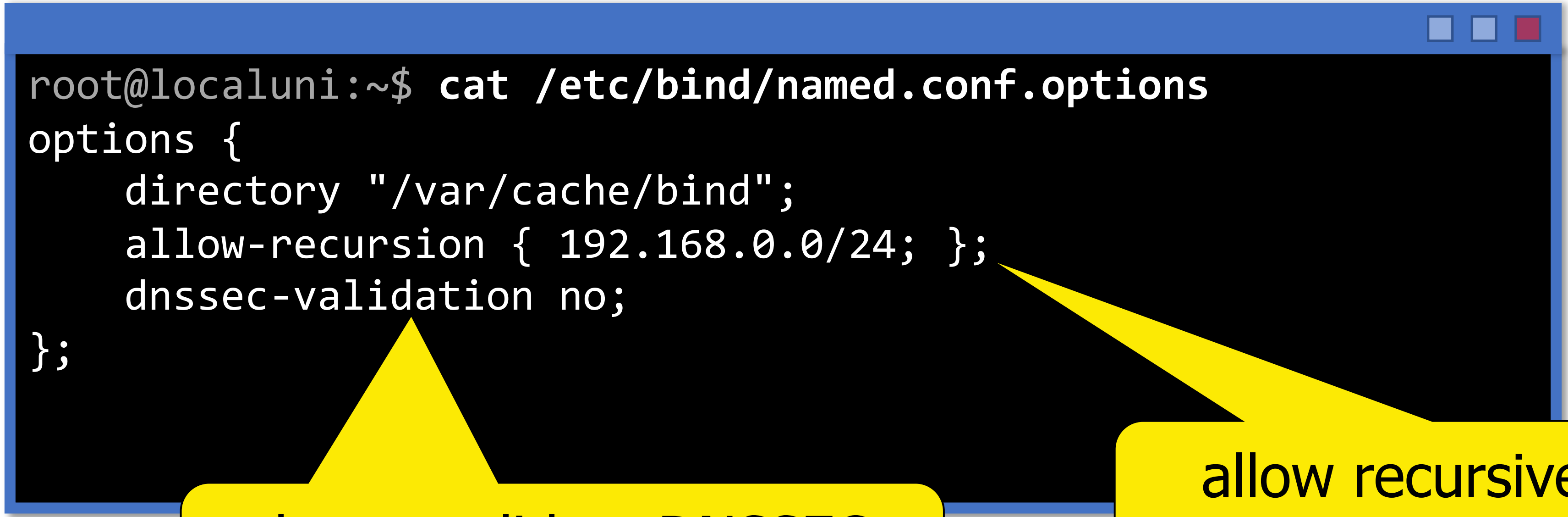
```
root@dnsit:~$ tail -n 5 /etc/bind/db.it
@                       IN      NS      dnsit.it.
dnsit.it.               IN      A       192.168.0.1

uniroma3.it.            IN      NS      dnsuni.uniroma3.it.
dnsuni.uniroma3.it.     IN      A       192.168.0.11
```

`dnsit.it` is the authority for this zone (**`it`**)

`dnsuni.uniroma3.it` is the authority for zone **`uniroma3(.it)`**

step 2 – exploring the configuration

- configuration on the name servers specifies
  - allowing recursive queries



```
root@localuni:~$ cat /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    allow-recursion { 192.168.0.0/24; };
    dnssec-validation no;
};
```

do not validate DNSSEC over the recursive queries

allow recursive queries from `192.168.0.0/24`

let’s start the lab