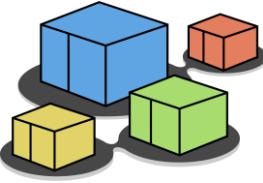




kathara lab

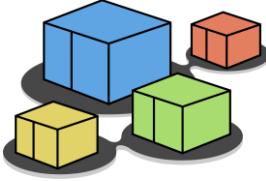
DNS

Version	2.2
Author(s)	L. Ariemma, T. Caiazzo, 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



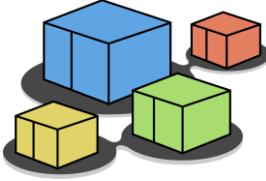
copyright notice

- 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.



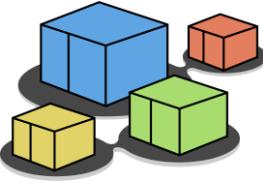
purpose of this lab

- get familiar with DNS
- observe the behavior of name servers and their interactions
- learn simple DNS configurations



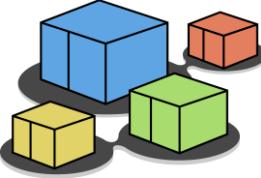
lab limitations

- DNS security issues and protocols are not covered
 - we use a version of Bind, which currently is the most widely used domain name server software, that allows ignoring security aspects



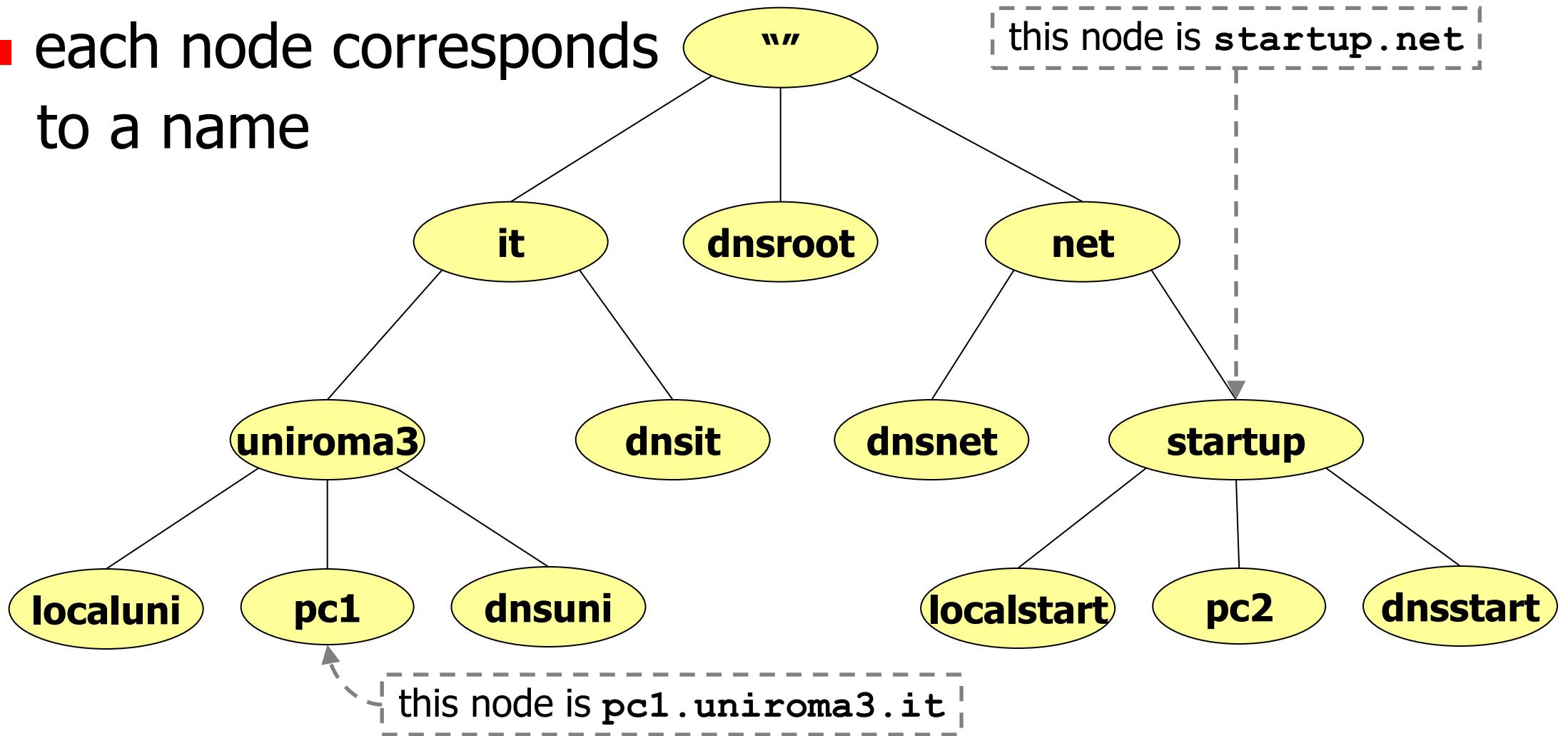
about the DNS

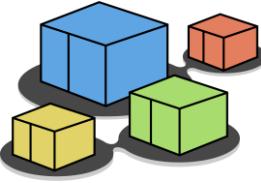
- takes care of associating names with IP addresses
- the **name system** is distributed over several nodes (hosts) that are hierarchically organized to form a tree
- each node in the hierarchy corresponds to a **name**
- a **domain** in the name system is a subtree
- a node in the hierarchy may be delegated 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

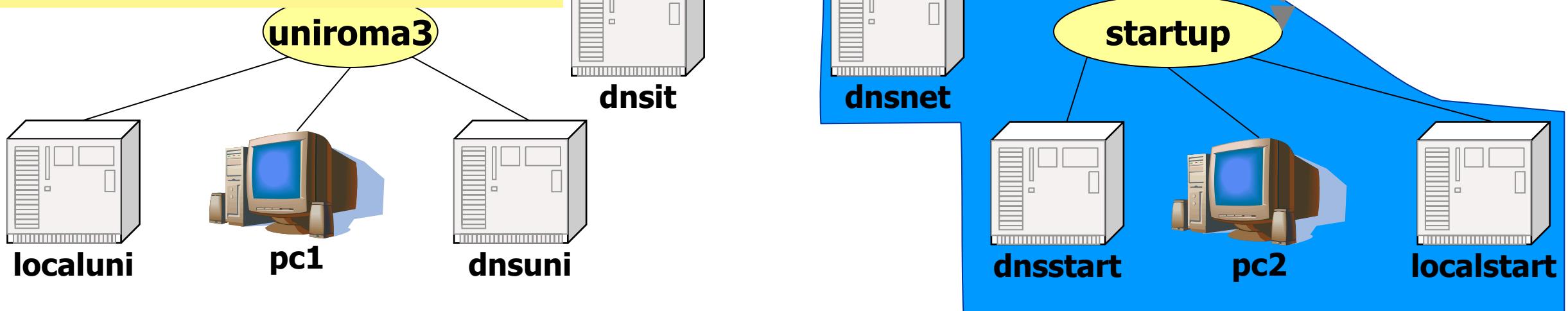
- each node corresponds to a name

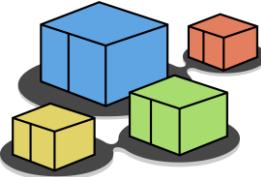




the DNS name hierarchy

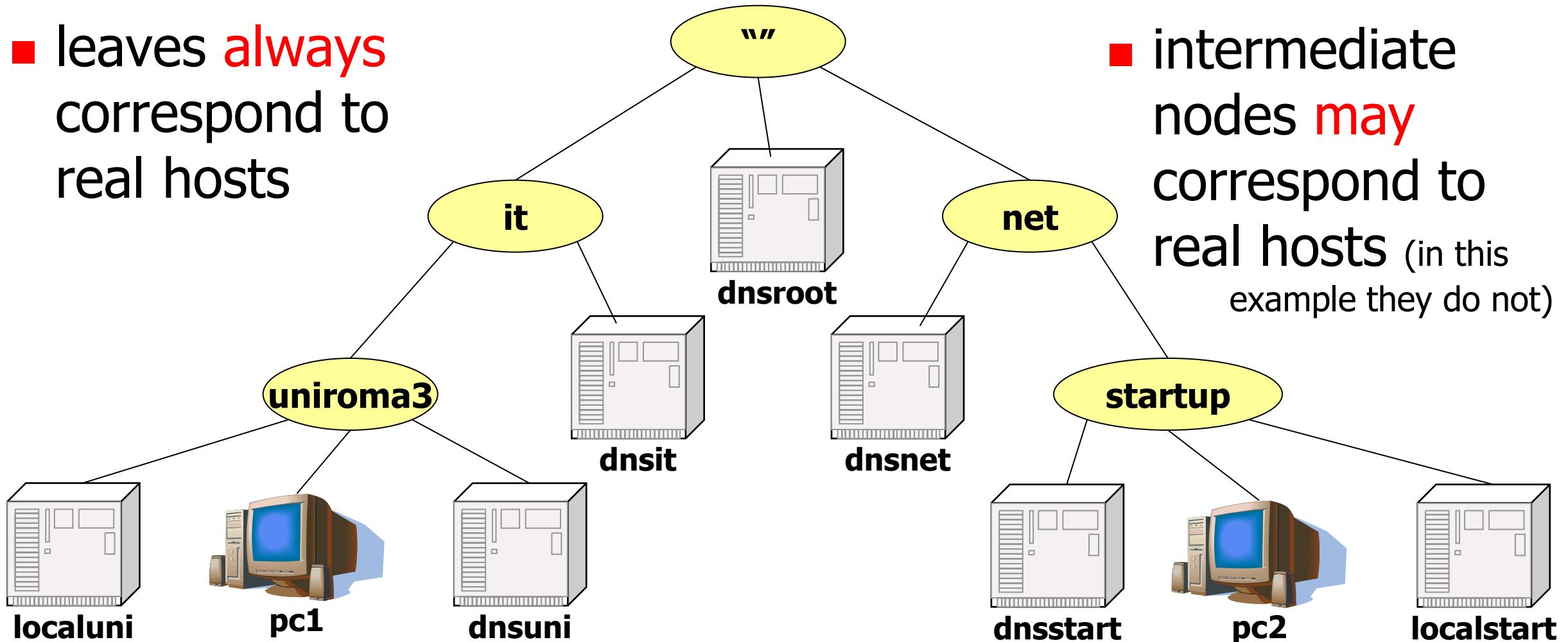
- domains are subtrees
 - their name is the name of the root node
 - every node (including leaves) defines a domain
 - domains do **overlap**



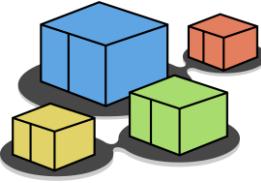


the DNS name hierarchy

- leaves **always** correspond to real hosts

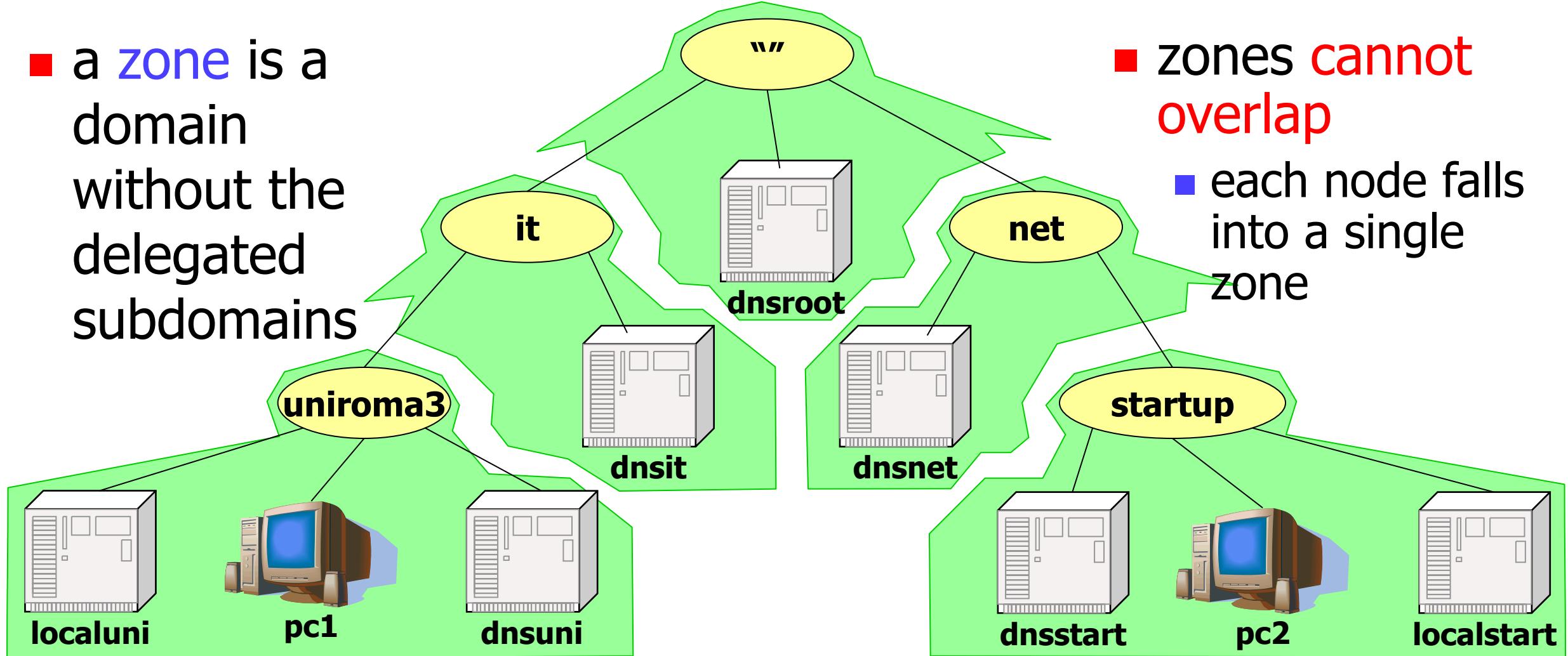


- intermediate nodes **may** correspond to real hosts (in this example they do not)

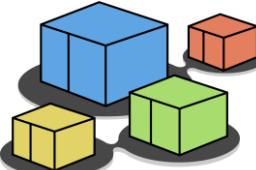


zones

- a **zone** is a domain without the delegated subdomains

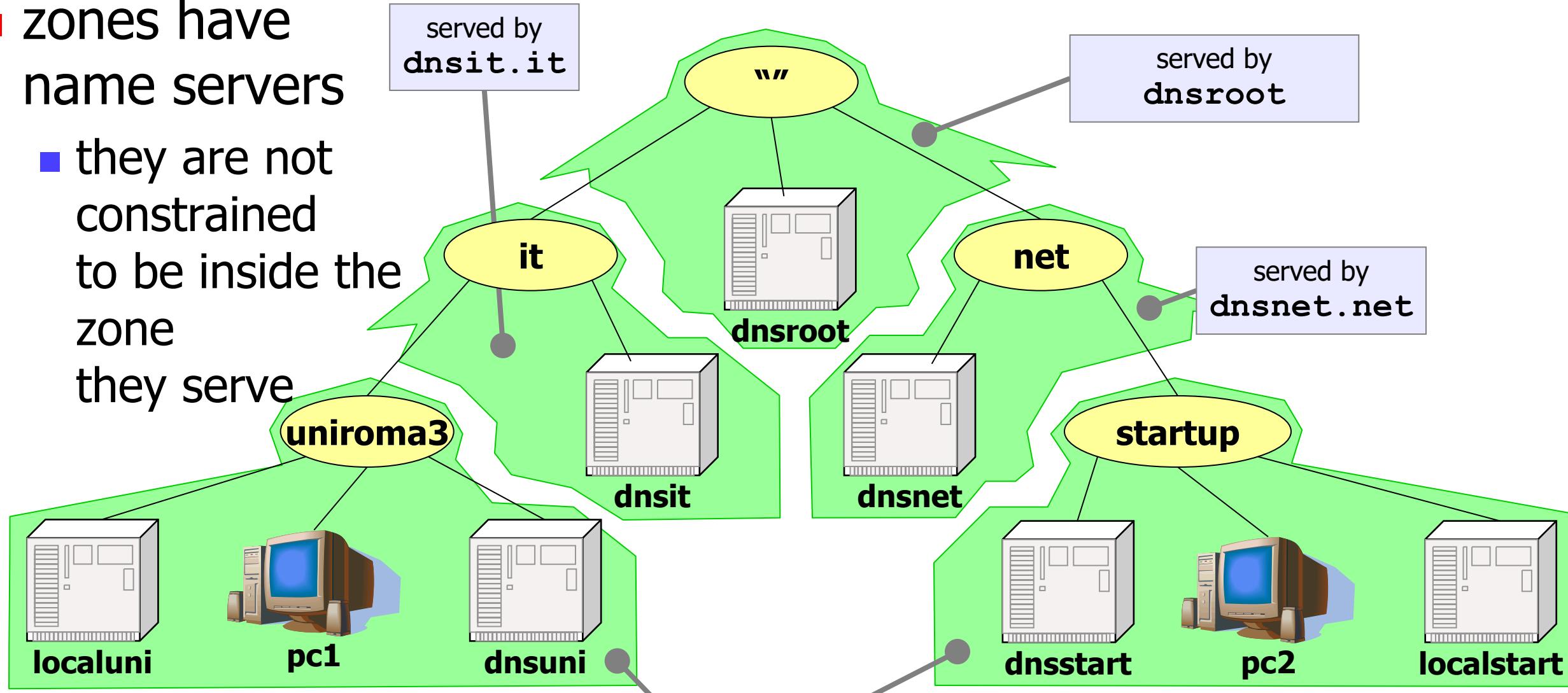


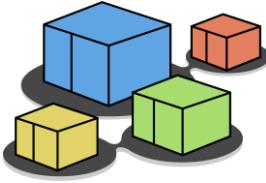
- **zones cannot overlap**
 - each node falls into a single zone



zones

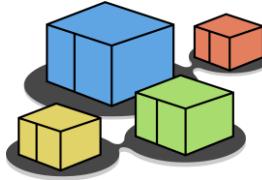
- zones have name servers
 - they are not constrained to be inside the zone they serve



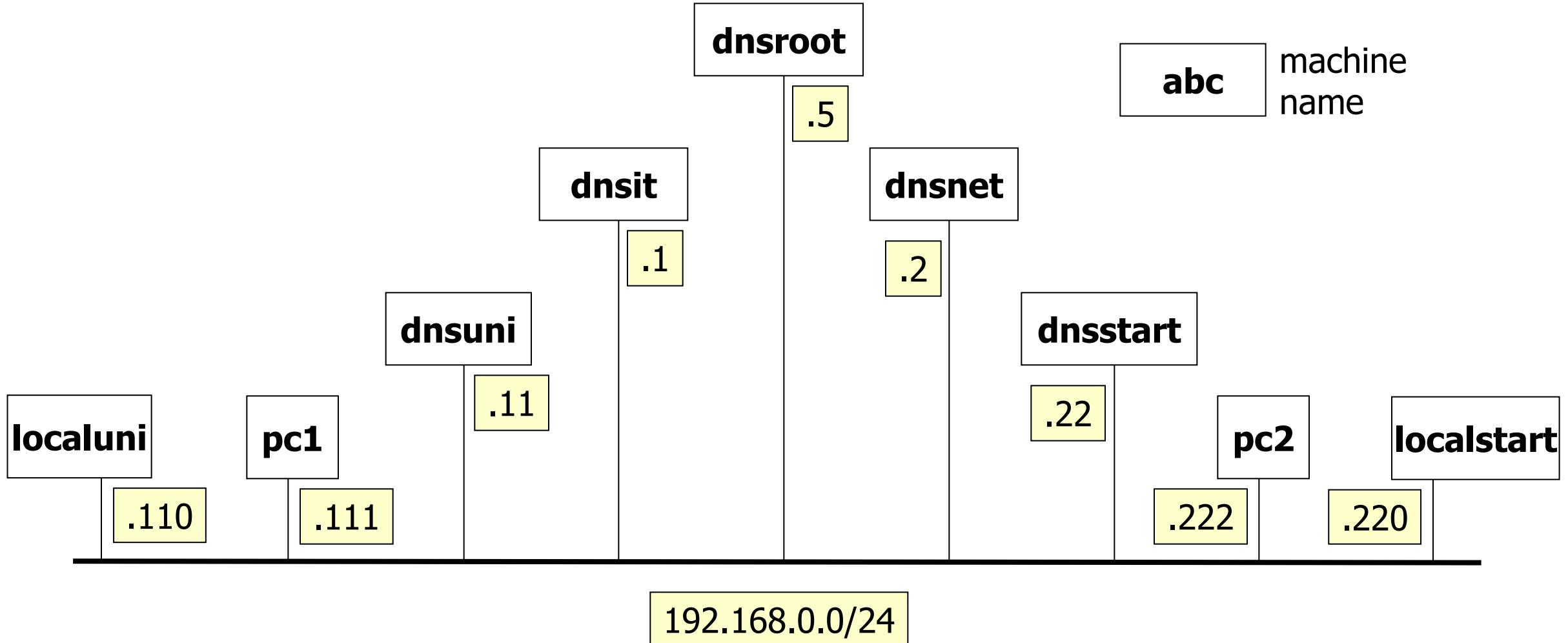


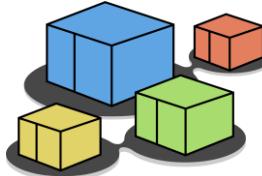
more about the DNS

- the dns hierarchy is largely 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

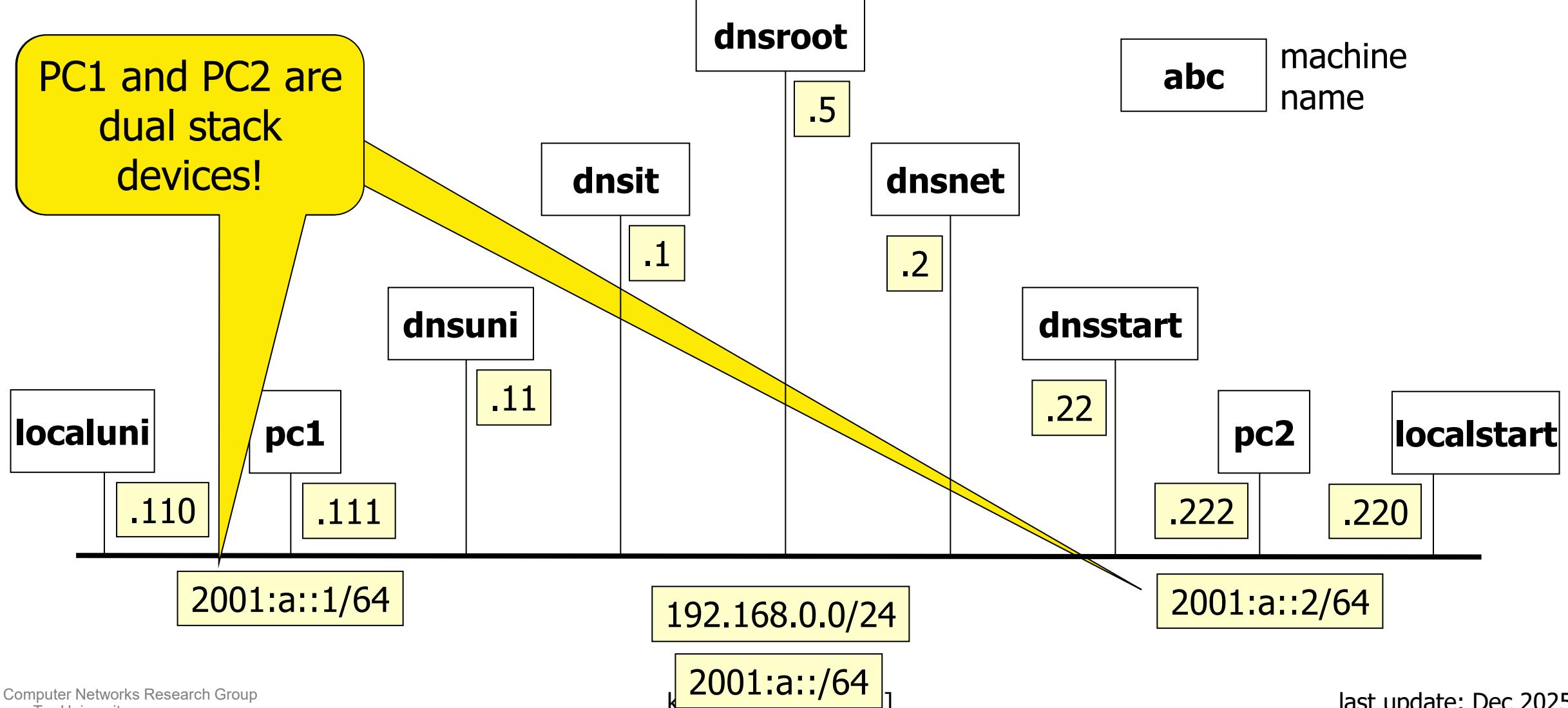


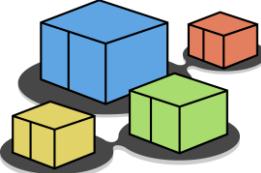
step 1 – network topology (lab.conf)



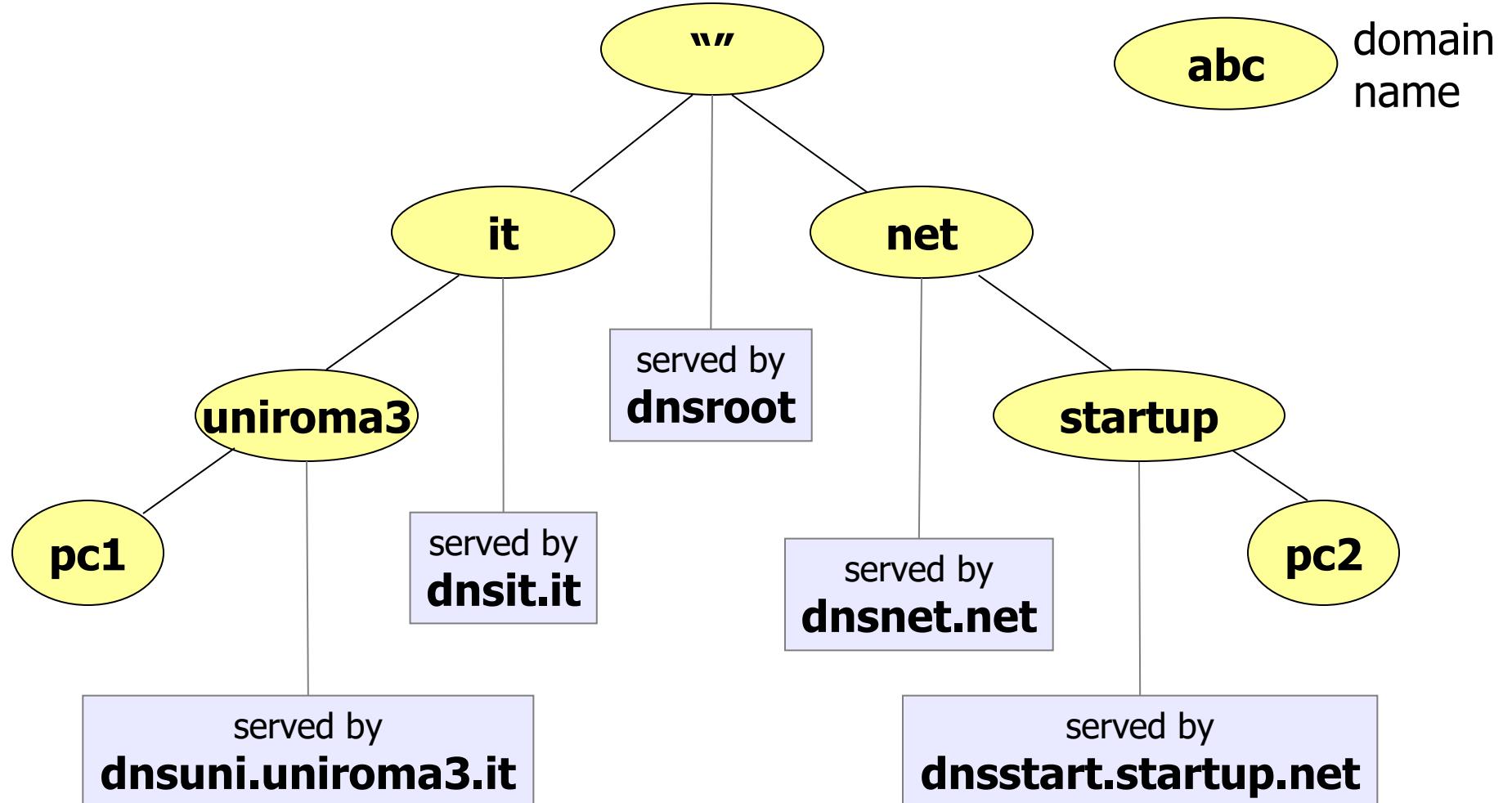


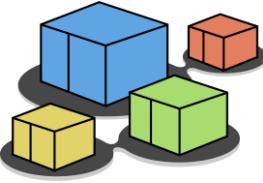
step 1 – network topology (lab.conf)





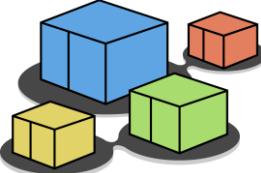
step 1 – DNS (zone) hierarchy





step 2 – starting the lab

- the lab is configured to
 - start all the 9 devices
 - automatically configure network interfaces (IPv4 only)
 - automatically configure the authoritative name servers
 - automatically configure name servers offering a recursive resolution service
 - automatically start the name server software (*bind*) on each name server
 - the daemon corresponding to bind is called *named*



step 2 – exploring the configuration

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

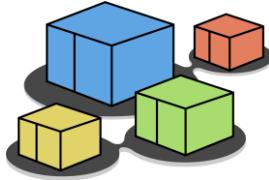
perform
first IPv4
and then
IPv6
queries

```
root@pc1:~$ cat /etc/resolv.conf
nameserver 192.168.0.110
options single-request
```

localuni.uniroma3.it

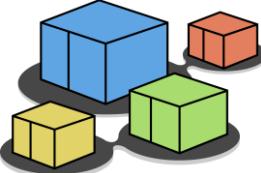
```
root@pc2:~$ cat /etc/resolv.conf
nameserver 192.168.0.220
options single-request
```

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

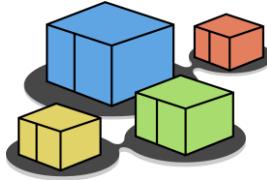
```
root@dnsuni:~$ cat /etc/bind/named.conf
include "/etc/bind/named.conf.options";  
  
zone "." {
    type hint;
    file "/etc/bind/db.root";
};  
  
zone "uniroma3.it" {
    type master;
    file "/etc/bind/db.it.uniroma3";
};
```

include some additional configuration

where to find information about the root name server

we are the primary master for zone **uniroma3.it**

where to find data about the names in this zone

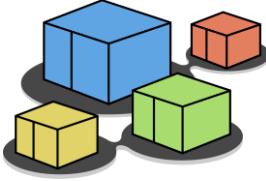


step 2 – exploring the configuration

- configuration on the name servers specifies
 - additional configuration

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

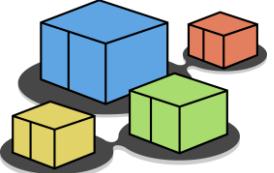
use this folder to store the cache.
COMPULSORY, otherwise, named wont 't start



format of a resource record

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

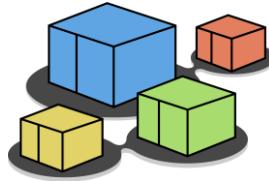
- domain: the record owner (=domain to which the record refers)
- class: usually IN (=Internet system); may be HS (=hesiod) or CH (=chaos)
- type: see next slide...
- rdata: record data (depends on the record type)



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

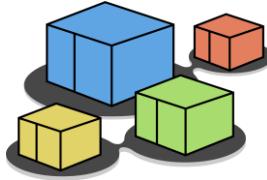


step 2 – exploring the configuration

- 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

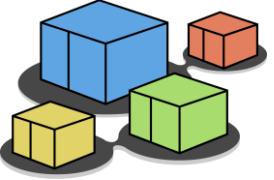


step 2 – exploring the configuration

- 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)



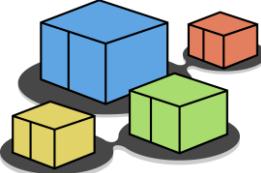
step 2 – exploring the configuration

- configuration on the name servers specifies
 - authoritative information

```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@           IN      SOA     dnsuni.uniroma3.it.
              root.dnsuni.uniroma3.it. (
                                2024120401 ; serial
                                28    ; refresh
                                14    ; retry
                                3600000 ; expire
                                0     ; negative cache ttl
                                )
```

- 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

Start of Authority record



step 2 – exploring the configuration

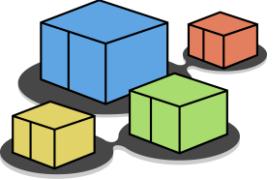
- configuration on the name servers specifies
 - authoritative information

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

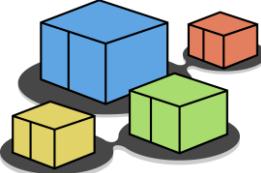


step 2 – exploring the configuration

- 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. (
                          20241201        serial
                          28 ;
```

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



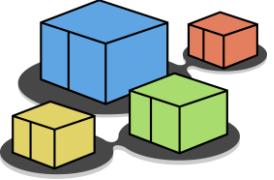
step 2 – exploring the configuration

- 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.  (
                                2024120401 ; serial
                                0 ; refresh
                                1800 ; expire
                                cache ttl
```

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

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

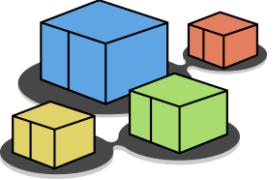


step 2 – exploring the configuration

- 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. (
                                2024120401 ; serial
                                28 ; refresh
                                14 ; retry
                                3600000 ; expire
                                0 ; negative cache ttl
)
```

makes sense for
master/slave server
configurations



step 2 – exploring the configuration

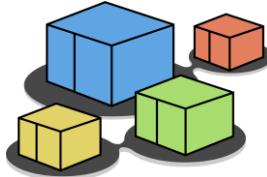
- configuration on the name servers specifies
 - authoritative information

```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@           IN      SOA     dnsuni.uniroma3.it.
              root dnsuni.uniroma3.it. (
                                2024120401 ; serial
                                28   ; refresh
                                14400 ; expire
                                3600  ; minimum)
```

serial number

2024120401 ; serial
28 ; refresh

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



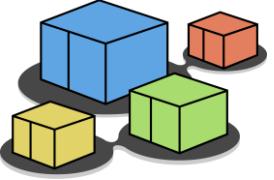
step 2 – exploring the configuration

- 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. (
                                2024120401 ; 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

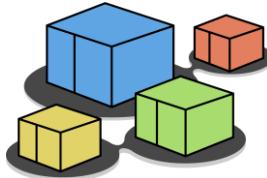


step 2 – exploring the configuration

- 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. (
                                2024120401 ; 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

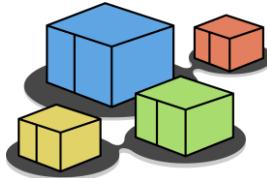
- configuration on the name servers specifies
 - authoritative information

```
root@dnsuni:~$ cat /etc/bind/db.it.uniroma3
$TTL    60000
@       IN SOA   ns1.it.uniroma3. hostmaster.it.uniroma3. 1 43200 7200 604800 86400
          IN NS    ns1.it.uniroma3.
          IN A     192.168.1.10
          IN MX   10 mail.it.uniroma3.
```

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

```
          IN A     192.168.1.11
          IN MX   10 mail2.it.uniroma3.
          IN NS    ns2.it.uniroma3.
          IN A     192.168.1.12
          IN MX   10 mail3.it.uniroma3.
          IN NS    ns3.it.uniroma3.
          IN A     192.168.1.13
          IN MX   10 mail4.it.uniroma3.
          IN NS    ns4.it.uniroma3.
          IN A     192.168.1.14
          IN MX   10 mail5.it.uniroma3.
          IN NS    ns5.it.uniroma3.
          IN A     192.168.1.15
          IN MX   10 mail6.it.uniroma3.
          IN NS    ns6.it.uniroma3.
          IN A     192.168.1.16
          IN MX   10 mail7.it.uniroma3.
          IN NS    ns7.it.uniroma3.
          IN A     192.168.1.17
          IN MX   10 mail8.it.uniroma3.
          IN NS    ns8.it.uniroma3.
          IN A     192.168.1.18
          IN MX   10 mail9.it.uniroma3.
          IN NS    ns9.it.uniroma3.
          IN A     192.168.1.19
          IN MX   10 mail10.it.uniroma3.
          IN NS   ns10.it.uniroma3.
          IN A     192.168.1.20
          IN MX   10 mail11.it.uniroma3.
          IN NS   ns11.it.uniroma3.
          IN A     192.168.1.21
          IN MX   10 mail12.it.uniroma3.
          IN NS   ns12.it.uniroma3.
          IN A     192.168.1.22
          IN MX   10 mail13.it.uniroma3.
          IN NS   ns13.it.uniroma3.
          IN A     192.168.1.23
          IN MX   10 mail14.it.uniroma3.
          IN NS   ns14.it.uniroma3.
          IN A     192.168.1.24
          IN MX   10 mail15.it.uniroma3.
          IN NS   ns15.it.uniroma3.
          IN A     192.168.1.25
          IN MX   10 mail16.it.uniroma3.
          IN NS   ns16.it.uniroma3.
          IN A     192.168.1.26
          IN MX   10 mail17.it.uniroma3.
          IN NS   ns17.it.uniroma3.
          IN A     192.168.1.27
          IN MX   10 mail18.it.uniroma3.
          IN NS   ns18.it.uniroma3.
          IN A     192.168.1.28
          IN MX   10 mail19.it.uniroma3.
          IN NS   ns19.it.uniroma3.
          IN A     192.168.1.29
          IN MX   10 mail20.it.uniroma3.
          IN NS   ns20.it.uniroma3.
          IN A     192.168.1.30
          IN MX   10 mail21.it.uniroma3.
          IN NS   ns21.it.uniroma3.
          IN A     192.168.1.31
          IN MX   10 mail22.it.uniroma3.
          IN NS   ns22.it.uniroma3.
          IN A     192.168.1.32
          IN MX   10 mail23.it.uniroma3.
          IN NS   ns23.it.uniroma3.
          IN A     192.168.1.33
          IN MX   10 mail24.it.uniroma3.
          IN NS   ns24.it.uniroma3.
          IN A     192.168.1.34
          IN MX   10 mail25.it.uniroma3.
          IN NS   ns25.it.uniroma3.
          IN A     192.168.1.35
          IN MX   10 mail26.it.uniroma3.
          IN NS   ns26.it.uniroma3.
          IN A     192.168.1.36
          IN MX   10 mail27.it.uniroma3.
          IN NS   ns27.it.uniroma3.
          IN A     192.168.1.37
          IN MX   10 mail28.it.uniroma3.
          IN NS   ns28.it.uniroma3.
          IN A     192.168.1.38
          IN MX   10 mail29.it.uniroma3.
          IN NS   ns29.it.uniroma3.
          IN A     192.168.1.39
          IN MX   10 mail30.it.uniroma3.
          IN NS   ns30.it.uniroma3.
          IN A     192.168.1.40
          IN MX   10 mail31.it.uniroma3.
          IN NS   ns31.it.uniroma3.
          IN A     192.168.1.41
          IN MX   10 mail32.it.uniroma3.
          IN NS   ns32.it.uniroma3.
          IN A     192.168.1.42
          IN MX   10 mail33.it.uniroma3.
          IN NS   ns33.it.uniroma3.
          IN A     192.168.1.43
          IN MX   10 mail34.it.uniroma3.
          IN NS   ns34.it.uniroma3.
          IN A     192.168.1.44
          IN MX   10 mail35.it.uniroma3.
          IN NS   ns35.it.uniroma3.
          IN A     192.168.1.45
          IN MX   10 mail36.it.uniroma3.
          IN NS   ns36.it.uniroma3.
          IN A     192.168.1.46
          IN MX   10 mail37.it.uniroma3.
          IN NS   ns37.it.uniroma3.
          IN A     192.168.1.47
          IN MX   10 mail38.it.uniroma3.
          IN NS   ns38.it.uniroma3.
          IN A     192.168.1.48
          IN MX   10 mail39.it.uniroma3.
          IN NS   ns39.it.uniroma3.
          IN A     192.168.1.49
          IN MX   10 mail40.it.uniroma3.
          IN NS   ns40.it.uniroma3.
          IN A     192.168.1.50
          IN MX   10 mail41.it.uniroma3.
          IN NS   ns41.it.uniroma3.
          IN A     192.168.1.51
          IN MX   10 mail42.it.uniroma3.
          IN NS   ns42.it.uniroma3.
          IN A     192.168.1.52
          IN MX   10 mail43.it.uniroma3.
          IN NS   ns43.it.uniroma3.
          IN A     192.168.1.53
          IN MX   10 mail44.it.uniroma3.
          IN NS   ns44.it.uniroma3.
          IN A     192.168.1.54
          IN MX   10 mail45.it.uniroma3.
          IN NS   ns45.it.uniroma3.
          IN A     192.168.1.55
          IN MX   10 mail46.it.uniroma3.
          IN NS   ns46.it.uniroma3.
          IN A     192.168.1.56
          IN MX   10 mail47.it.uniroma3.
          IN NS   ns47.it.uniroma3.
          IN A     192.168.1.57
          IN MX   10 mail48.it.uniroma3.
          IN NS   ns48.it.uniroma3.
          IN A     192.168.1.58
          IN MX   10 mail49.it.uniroma3.
          IN NS   ns49.it.uniroma3.
          IN A     192.168.1.59
          IN MX   10 mail50.it.uniroma3.
          IN NS   ns50.it.uniroma3.
          IN A     192.168.1.60
          IN MX   10 mail51.it.uniroma3.
          IN NS   ns51.it.uniroma3.
          IN A     192.168.1.61
          IN MX   10 mail52.it.uniroma3.
          IN NS   ns52.it.uniroma3.
          IN A     192.168.1.62
          IN MX   10 mail53.it.uniroma3.
          IN NS   ns53.it.uniroma3.
          IN A     192.168.1.63
          IN MX   10 mail54.it.uniroma3.
          IN NS   ns54.it.uniroma3.
          IN A     192.168.1.64
          IN MX   10 mail55.it.uniroma3.
          IN NS   ns55.it.uniroma3.
          IN A     192.168.1.65
          IN MX   10 mail56.it.uniroma3.
          IN NS   ns56.it.uniroma3.
          IN A     192.168.1.66
          IN MX   10 mail57.it.uniroma3.
          IN NS   ns57.it.uniroma3.
          IN A     192.168.1.67
          IN MX   10 mail58.it.uniroma3.
          IN NS   ns58.it.uniroma3.
          IN A     192.168.1.68
          IN MX   10 mail59.it.uniroma3.
          IN NS   ns59.it.uniroma3.
          IN A     192.168.1.69
          IN MX   10 mail60.it.uniroma3.
          IN NS   ns60.it.uniroma3.
          IN A     192.168.1.70
          IN MX   10 mail61.it.uniroma3.
          IN NS   ns61.it.uniroma3.
          IN A     192.168.1.71
          IN MX   10 mail62.it.uniroma3.
          IN NS   ns62.it.uniroma3.
          IN A     192.168.1.72
          IN MX   10 mail63.it.uniroma3.
          IN NS   ns63.it.uniroma3.
          IN A     192.168.1.73
          IN MX   10 mail64.it.uniroma3.
          IN NS   ns64.it.uniroma3.
          IN A     192.168.1.74
          IN MX   10 mail65.it.uniroma3.
          IN NS   ns65.it.uniroma3.
          IN A     192.168.1.75
          IN MX   10 mail66.it.uniroma3.
          IN NS   ns66.it.uniroma3.
          IN A     192.168.1.76
          IN MX   10 mail67.it.uniroma3.
          IN NS   ns67.it.uniroma3.
          IN A     192.168.1.77
          IN MX   10 mail68.it.uniroma3.
          IN NS   ns68.it.uniroma3.
          IN A     192.168.1.78
          IN MX   10 mail69.it.uniroma3.
          IN NS   ns69.it.uniroma3.
          IN A     192.168.1.79
          IN MX   10 mail70.it.uniroma3.
          IN NS   ns70.it.uniroma3.
          IN A     192.168.1.80
          IN MX   10 mail71.it.uniroma3.
          IN NS   ns71.it.uniroma3.
          IN A     192.168.1.81
          IN MX   10 mail72.it.uniroma3.
          IN NS   ns72.it.uniroma3.
          IN A     192.168.1.82
          IN MX   10 mail73.it.uniroma3.
          IN NS   ns73.it.uniroma3.
          IN A     192.168.1.83
          IN MX   10 mail74.it.uniroma3.
          IN NS   ns74.it.uniroma3.
          IN A     192.168.1.84
          IN MX   10 mail75.it.uniroma3.
          IN NS   ns75.it.uniroma3.
          IN A     192.168.1.85
          IN MX   10 mail76.it.uniroma3.
          IN NS   ns76.it.uniroma3.
          IN A     192.168.1.86
          IN MX   10 mail77.it.uniroma3.
          IN NS   ns77.it.uniroma3.
          IN A     192.168.1.87
          IN MX   10 mail78.it.uniroma3.
          IN NS   ns78.it.uniroma3.
          IN A     192.168.1.88
          IN MX   10 mail79.it.uniroma3.
          IN NS   ns79.it.uniroma3.
          IN A     192.168.1.89
          IN MX   10 mail80.it.uniroma3.
          IN NS   ns80.it.uniroma3.
          IN A     192.168.1.90
          IN MX   10 mail81.it.uniroma3.
          IN NS   ns81.it.uniroma3.
          IN A     192.168.1.91
          IN MX   10 mail82.it.uniroma3.
          IN NS   ns82.it.uniroma3.
          IN A     192.168.1.92
          IN MX   10 mail83.it.uniroma3.
          IN NS   ns83.it.uniroma3.
          IN A     192.168.1.93
          IN MX   10 mail84.it.uniroma3.
          IN NS   ns84.it.uniroma3.
          IN A     192.168.1.94
          IN MX   10 mail85.it.uniroma3.
          IN NS   ns85.it.uniroma3.
          IN A     192.168.1.95
          IN MX   10 mail86.it.uniroma3.
          IN NS   ns86.it.uniroma3.
          IN A     192.168.1.96
          IN MX   10 mail87.it.uniroma3.
          IN NS   ns87.it.uniroma3.
          IN A     192.168.1.97
          IN MX   10 mail88.it.uniroma3.
          IN NS   ns88.it.uniroma3.
          IN A     192.168.1.98
          IN MX   10 mail89.it.uniroma3.
          IN NS   ns89.it.uniroma3.
          IN A     192.168.1.99
          IN MX   10 mail90.it.uniroma3.
          IN NS   ns90.it.uniroma3.
          IN A     192.168.1.100
          IN MX   10 mail91.it.uniroma3.
          IN NS   ns91.it.uniroma3.
          IN A     192.168.1.101
          IN MX   10 mail92.it.uniroma3.
          IN NS   ns92.it.uniroma3.
          IN A     192.168.1.102
          IN MX   10 mail93.it.uniroma3.
          IN NS   ns93.it.uniroma3.
          IN A     192.168.1.103
          IN MX   10 mail94.it.uniroma3.
          IN NS   ns94.it.uniroma3.
          IN A     192.168.1.104
          IN MX   10 mail95.it.uniroma3.
          IN NS   ns95.it.uniroma3.
          IN A     192.168.1.105
          IN MX   10 mail96.it.uniroma3.
          IN NS   ns96.it.uniroma3.
          IN A     192.168.1.106
          IN MX   10 mail97.it.uniroma3.
          IN NS   ns97.it.uniroma3.
          IN A     192.168.1.107
          IN MX   10 mail98.it.uniroma3.
          IN NS   ns98.it.uniroma3.
          IN A     192.168.1.108
          IN MX   10 mail99.it.uniroma3.
          IN NS   ns99.it.uniroma3.
          IN A     192.168.1.109
          IN MX   10 mail100.it.uniroma3.
          IN NS   ns100.it.uniroma3.
```

slave expire time
(seconds)

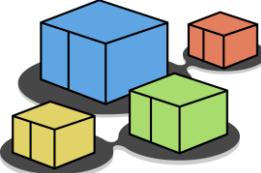


step 2 – exploring the configuration

- 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. (
                                2024120401 ; serial
                                28    ; refresh
                                14    ; retry
                                3600000 ; expire
                                0     ; negative cache ttl
              )
```

ttl for negative responses from authoritative name servers



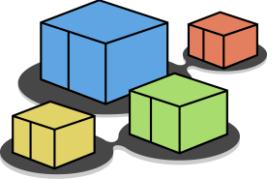
step 2 – exploring the configuration

- 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.
                         .       3.it. (
                         .       2024120401 ; serial
                         .       28 ; refresh
                         .       14 ; retry
                         .       3600000 ; expire
                         .       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
pc1.uniroma3.it.      IN      AAAA    2001:a::1
```

record type NS
(name server)

the authoritative name server for
this zone (**uniroma3.it**) is
dnsuni.uniroma3.it

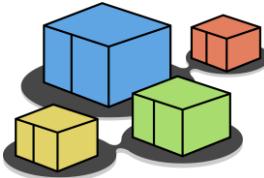


step 2 – exploring the configuration

- 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. (
                                2024120401 ; serial
                                28      ; refresh
                                14      ; retry
                                3600000 ; expire
                                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
pc1.uniroma3.it.     IN      AAAA   2001:a::1
```

record type A
(IPv4 address)



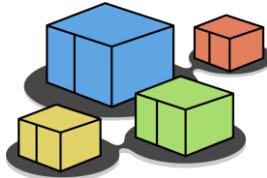
step 2 – exploring the configuration

- 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. (
                                2024120401 ; serial
                                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
pc1.uniroma3.it.     IN      AAAA   2001:a::1
```

record type AAAA
(IPv6 address)

two machines in this zone:
`dnsuni.uniroma3.it`
`pc1.uniroma3.it`



step 2 – exploring the configuration

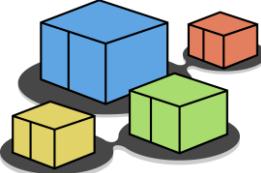
- configuration on the name servers specifies
 - associations between names and ip addresses

```
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

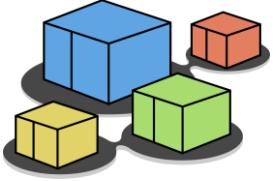
- configuration on the name servers specifies
 - allowing recursive queries and disabling dnssec

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

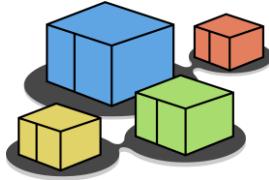
disable
dnssec

allow recursive queries
from 192.168.0.0/24

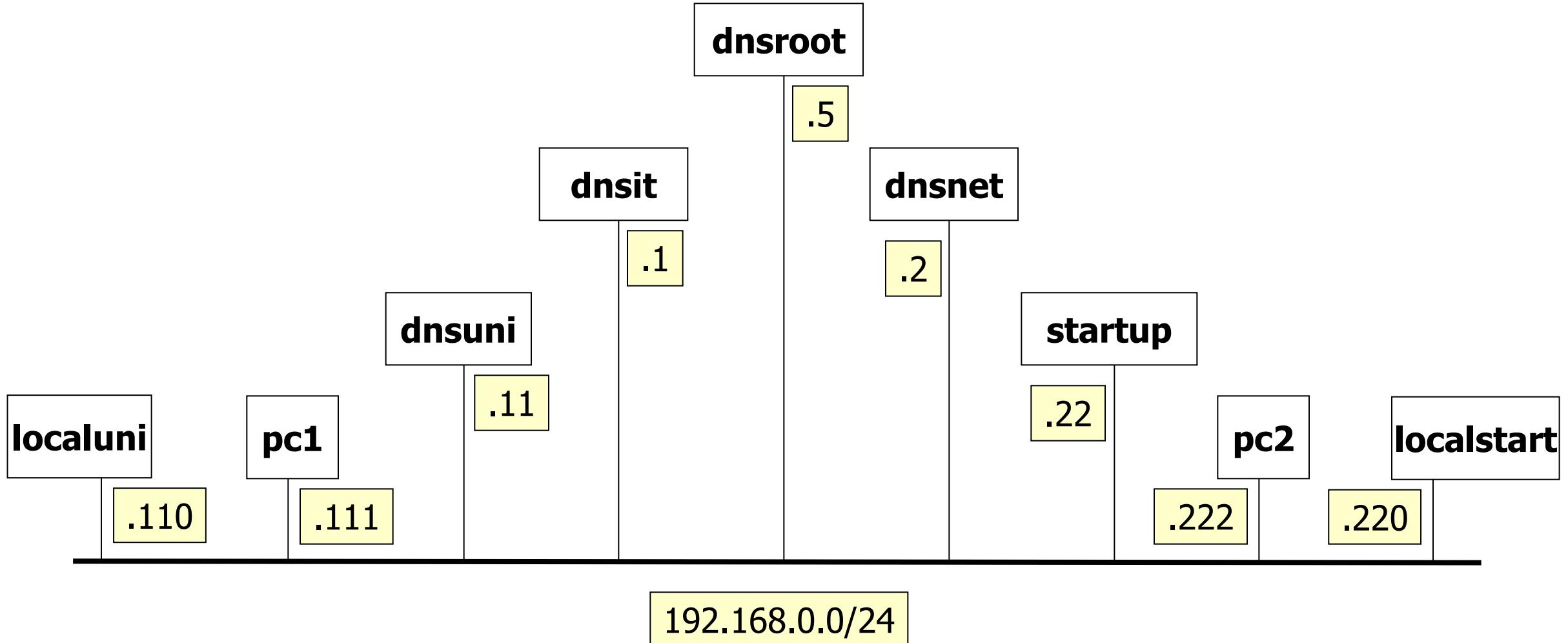
Do not send
DNS cookies

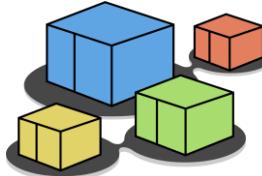


let's start the lab

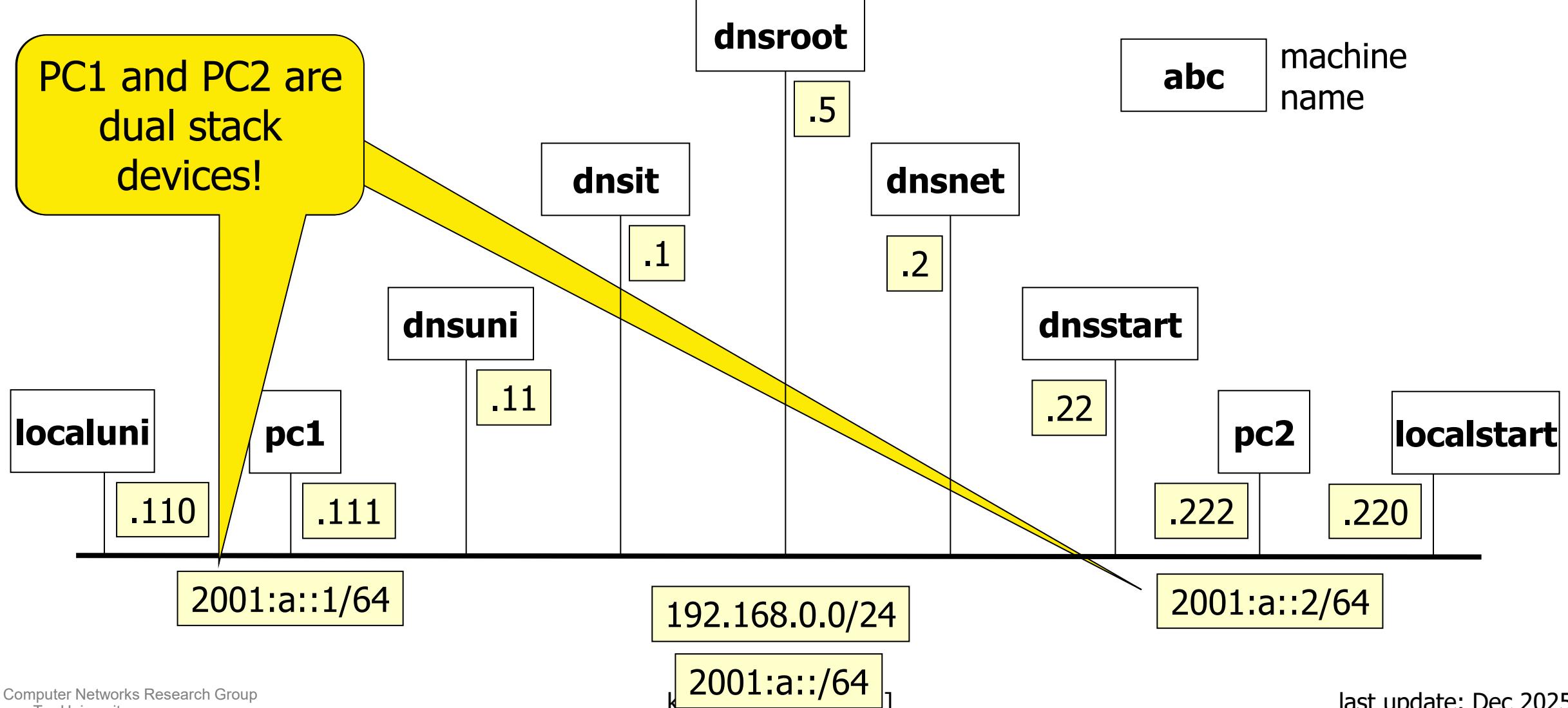


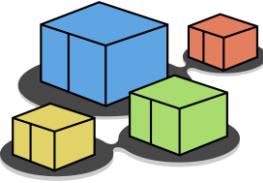
step 3 – experiment setting





step 1 – network topology (lab.conf)



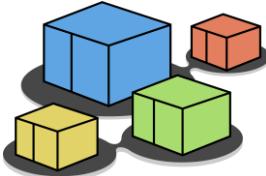


sniff the traffic

- connect the wireshark device to collision domain A

```
user@localhost:~/kathara-lab_dns$ kathara lconfig -n wireshark --add A
```

- open any browser on the host machine
 - on **localhost:3000**
 - sniff eth1



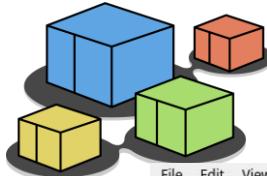
step 3 – ping from pc1

- execute a ping command towards pc2

Numeric output only. No attempt will be made to lookup symbolic names for host addresses.

pc1

```
root@pc1:/# ping4 -n pc2.startup.net
PING pc2.startup.net (192.168.0.222) 56(84) bytes of data.
64 bytes from 192.168.0.222: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 192.168.0.222: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.0.222: icmp_seq=3 ttl=64 time=0.525 ms
--- pc2.startup.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.525/0.867/1.496/0.445 ms
```



ste

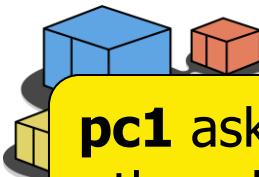
filter to only
show DNS
packets

sniffer output

No.	Time	Source	Destination	Information
3	0.000...	192.168.0.111	192.168.0.110	3 0.000... 192.168.0.111 192.168.0.110 DNS 86 Standard query 0xeabd A pc2.startup.net OPT
6	0.002...	192.168.0.110	192.168.0.5	6 0.002... 192.168.0.110 192.168.0.5 DNS 86 Standard query 0xeabd A pc2.startup.net OPT
7	0.002...	192.168.0.110	192.168.0.5	7 0.002... 192.168.0.110 192.168.0.5 DNS 70 Standard query 0x3352 NS <Root> OPT
8	0.002...	192.168.0.5	192.168.0.110	8 0.002... 192.168.0.5 192.168.0.110 DNS 123 Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
10	0.003...	192.168.0.5	192.168.0.110	10 0.003... 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12	0.004...	192.168.0.110	192.168.0.2	12 0.004... 192.168.0.110 192.168.0.2 DNS 86 Standard query 0x77b7 A pc2.startup.net OPT
13	0.004...	192.168.0.2	192.168.0.110	13 0.004... 192.168.0.2 192.168.0.110 DNS 125 Standard query response 0x77b7 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.2...
16	0.006...	192.168.0.110	192.168.0.22	16 0.006... 192.168.0.110 192.168.0.22 DNS 86 Standard query 0x708f A pc2.startup.net OPT
17	0.006...	192.168.0.22	192.168.0.110	17 0.006... 192.168.0.22 192.168.0.110 DNS 102 Standard query response 0x708f A pc2.startup.net A 192.168.0.222 OPT
18	0.007...	192.168.0.110	192.168.0.111	18 0.007... 192.168.0.110 192.168.0.111 DNS 130 Standard query response 0x7e04 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.n...
19	0.007...	192.168.0.111	192.168.0.110	19 0.007... 192.168.0.111 192.168.0.110 DNS 75 Standard query 0x7608 AAAA pc2.startup.net
20	0.008...	192.168.0.110	192.168.0.22	20 0.008... 192.168.0.110 192.168.0.22 DNS 86 Standard query 0xffe6 AAAA pc2.startup.net OPT
21	0.009...	192.168.0.22	192.168.0.110	21 0.009... 192.168.0.22 192.168.0.110 DNS 153 Standard query response 0xffe6 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...
22	0.009...	192.168.0.110	192.168.0.111	22 0.009... 192.168.0.110 192.168.0.111 DNS 142 Standard query response 0x7608 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
Ethernet II, Src: f2:84:08:67:54:3c (f2:84:08:67:54:3c), Dst: ba:62:
Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110
User Datagram Protocol, Src Port: 44329, Dst Port: 53
Domain Name System (query)

0000	ba	62	ca	b2	e5	d4	f2	84	08	67	54	3c	08	00	45	00	.b.....g
0010	00	3d	11	df	40	00	40	11	a6	a3	c0	a8	00	6f	c0	a8	=@. @. .
0020	00	6e	ad	29	00	35	00	29	1b	cc	7e	04	01	00	00	01	.n.)5.) .
0030	00	00	00	00	00	00	03	70	63	32	07	73	74	61	72	74p c2
0040	75	70	03	6e	65	74	00	00	01	00	01						up.net...



pc1 asks to localuni
the address of pc2

step 3 – the sniffer output

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000...	192.168.0.111	192.168.0.110	DNS	75	Standard query 0x7e04 A pc2.startup.net
6	0.002...	192.168.0.110	192.168.0.5	DNS	86	Standard query 0xeabd A pc2.startup.net OPT
7	0.002...	192.168.0.110	192.168.0.5	DNS	70	Standard query 0x3352 NS <Root> OPT
8	0.002...	192.168.0.5	192.168.0.110	DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
10	0.003...	192.168.0.5	192.168.0.110	DNS	102	Standard query response 0x3352 NS <Root> NS SERVER A 192.168.0.5 OPT
12	0.004...	192.168.0.110	192.168.0.2	DNS	77	Standard query response 7b7 A pc2.startup.net OPT
13	0.004...	192.168.0.2	192.168.0.110	DNS	77	Standard query response 77b7 A pc2.startup.net OPT
16	0.006...	192.168.0.110	192.168.0.22	DNS	80	Standard query 0x08f A pc2.startup.net OPT
17	0.006...	192.168.0.22	192.168.0.110	DNS	102	Standard query response 0x08f A pc2.startup.net OPT
18	0.007...	192.168.0.110	192.168.0.111	DNS	130	Standard query response 0x08f A pc2.startup.net OPT
19	0.007...	192.168.0.111	192.168.0.110	DNS	75	Standard query 0x7608 A pc2.startup.net
20	0.008...	192.168.0.110	192.168.0.22	DNS	86	Standard query 0xffed A pc2.startup.net OPT
21	0.009...	192.168.0.22	192.168.0.110	DNS	153	Standard query response AA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...
22	0.009...	192.168.0.110	192.168.0.111	DNS	142	Standard query response AA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...

query id

query value

query type
(address)

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured

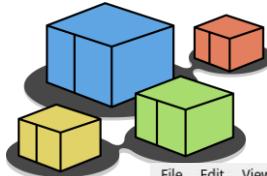
Ethernet II, Src: f2:84:08:67:54:3c (f2:84:08:67:54:3c), Dst: 192.168.0.110 (00:0c:29:00:00:00)

Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110 (00:0c:29:00:00:00)

User Datagram Protocol, Src Port: 44329, Dst Port: 53

Domain Name System (query)

b2 e5 d4 f2 84 08 67 54 3c 08 00 45 00 .b.....g
df 40 00 40 11 a6 a3 c0 a8 00 6f c0 a8 .=@. @...
0020 00 6e ad 29 00 35 00 29 1b cc 7e 04 01 00 00 01 .n.) 5.) ...
0030 00 00 00 00 00 00 03 70 63 32 07 73 74 61 72 74p c2
0040 75 70 03 6e 65 74 00 00 01 00 01 up.net... .



step 3 – the sniffer output

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000...	192.168.0.111	192.168.0.110	DNS	75	Standard query 0x7e04 A pc2.startup.net
6	0.002...	192.168.0.110	192.168.0.5	DNS	86	Standard query 0xeabd A pc2.startup.net OPT
7	0.002...	192.168.0.110	192.168.0.5	DNS	70	Standard query 0x3352 NS <Root> OPT
8	0.002...	192.168.0.5	192.168.0.110	DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
10	0.003...	192.168.0.5	192.168.0.110	DNS	110	Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12	0.004...	192.168.0.110	192.168.0.2	DNS	86	Standard query 0x77b7 A pc2.startup.net OPT
13	0.004...	192.168.0.2	192.168.0.110	DNS	125	Standard query response 0x77b7 A pc2.startup.net
16	0.006...	192.168.0.110	192.168.0.22	DNS	86	Standard query 0x708f A pc2.startup.net OPT
17	0.006...	192.168.0.22	192.168.0.110	DNS	102	Standard query response 0x708f A pc2.startup.net A 192.
18	0.007...	192.168.0.110	192.168.0.111	DNS	130	Standard query response 0x7e04 A pc2.startup.net A 192.
19	0.007...	192.168.0.111	192.168.0.110	DNS	75	Standard query 0x7608 AAAA pc2.startup.net
20	0.008...	192.168.0.110	192.168.0.22	DNS	86	Standard query 0xffe6 AAAA pc2.startup.net OPT
21	0.009...	192.168.0.22	192.168.0.110	DNS	153	Standard query response 0xffe6 AAAA pc2.startup.net AAAA
22	0.009...	192.168.0.110	192.168.0.111	DNS	142	Standard query response 0x7608 AAAA pc2.startup.net AAAA

```
› Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) c  
› Ethernet II, Src: f2:84:08:67:54:3c (f2:84:08:67:54:3c), Dst: ba:62:  
› Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110  
› User Datagram Protocol, Src Port: 44329, Dst Port: 53  
› Domain Name System (query)
```

0000	ba	62	ca	b2	e5	d4	f2	84	08	67	54	3c	08	00	45	00	.b.....g
0010	00	3d	11	df	40	00	40	11	a6	a3	c0	a8	00	6f	c0	a8	=@. @. .
0020	00	6e	ad	29	00	35	00	29	1b	cc	7e	04	01	00	00	01	.n.)5.) .
0030	00	00	00	00	00	00	03	70	63	32	07	73	74	61	72	74p c2
0040	75	70	03	6e	65	74	00	00	01	00	01						up.net...

request root name servers

answer with all the authoritative root name servers



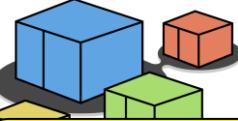
localuni asks **dnsroot**
who is the name server
for the **net** domain

Step 3 – the sniffer output

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000...	192.168.0.110	192.168.0.110	DNS	75	Standard query 0x7e04 A pc2.startup.net
6	0.002...	192.168.0.110	192.168.0.5	DNS	86	Standard query 0xeabd A pc2.startup.net OPT
7	0.002...	192.168.0.110	192.168.0.5	DNS	70	Standard query 0x3352 NS <Root> OPT
8	0.002...	192.168.0.5	192.168.0.110	DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
10	0.003...	192.168.0.5	192.168.0.110	DNS	110	Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12	0.004...	192.168.0.110	192.168.0.2	DNS	86	Standard query 0x77b7 A pc2.startup.net OPT
			110	DNS	125	Standard query response 0x77b7 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.2...
			22	DNS	86	Standard query 0x708f A pc2.startup.net OPT
			110	DNS	102	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 OPT
			111	DNS	130	Standard query response 0x7e04 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.n...
			110	DNS	75	Standard query 0x7608 AAAA pc2.startup.net
			20	DNS	86	Standard query 0xffe6 AAAA pc2.startup.net OPT
21	0.009...	192.168.0.22	192.168.0.110	DNS	153	Standard query response 0xffe6 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...
22	0.009...	192.168.0.110	192.168.0.111	DNS	142	Standard query response 0x7608 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup...

- Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
- Ethernet II, Src: ba:62:ca:b2:e5:d4 (ba:62:ca:b2:e5:d4), Dst: 42:af:00 (eth0)
- Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.5
- User Datagram Protocol, Src Port: 57254, Dst Port: 53
- Domain Name System (query)

0000	42	af	96	11	88	22	ba	62	ca	b2	e5	d4	08	00	45	00	B....."·b ..
0010	00	48	ee	3f	00	00	40	11	0a	a2	c0	a8	00	6e	c0	a8	.H..?..@. . .
0020	00	05	df	a6	00	35	00	34	fb	ae	ea	bd	00	10	00	015·4 ..
0030	00	00	00	00	00	01	03	70	63	32	07	73	74	61	72	74p c2 ..
0040	75	70	03	6e	65	74	00	00	01	00	01	00	00	29	02	00	up.net... . . .
0050	00	00	80	00	00	00	00	00	00	00	00	00	00	00	00	00



step 3 – the sniffer output

localuni asks dnsnet who is the name server for the **startup.net** domain

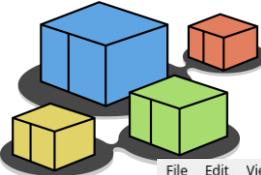
7 0.0024...	192.168.0.5	92.168.0.5
8 0.0026...	192.168.0.7	92.168.0.110
10 0.0033...	192.168.0.5	92.168.0.110
12 0.0040...	192.168.0.110	192.168.0.2
13 0.0049...	192.168.0.2	192.168.0.110
16 0.0060...	192.168.0.110	192.168.0.22
17 0.0065...	192.168.0.22	192.168.0.110
18 0.0072...	192.168.0.110	192.168.0.111
19 0.0076...	192.168.0.111	192.168.0.110
20 0.0084...	192.168.0.110	192.168.0.22
21 0.0090...	192.168.0.22	192.168.0.110
22 0.0093...	192.168.0.110	192.168.0.111

dnsstart.startup.net
address is 192.168.0.22

Protocol	Length	Info
110 DNS	75	Standard query 0x7e04 A pc2.startup.net
.5 DNS	86	Standard query 0xeabd A pc2.startup.net OPT
70 DNS	70	Standard query 0x3352 NS <Root> OPT
123 DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
110 DNS	110	Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.0040... 192.168.0.110 192.168.0.2 DNS	86	Standard query 0x77b7 A pc2.startup.net OPT
13 0.0049... 192.168.0.2 192.168.0.110 DNS	125	Standard query response 0x77b7 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
16 0.0060... 192.168.0.110 192.168.0.22 DNS	86	Standard query 0x708f A pc2.startup.net OPT
17 0.0065... 192.168.0.22 192.168.0.110 DNS	102	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 OPT
18 0.0072... 192.168.0.110 192.168.0.111 DNS	122	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...
19 0.0076... 192.168.0.111 192.168.0.110 DNS	122	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...
20 0.0084... 192.168.0.110 192.168.0.22 DNS	122	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...
21 0.0090... 192.168.0.22 192.168.0.110 DNS	122	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...
22 0.0093... 192.168.0.110 192.168.0.111 DNS	122	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...

```
▶ Frame 12: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on int
  ▶ Ethernet II, Src: ba:62:ca:b2:e5:d4 (ba:62:ca:b2:e5:d4), Dst: 4a:30:fe:65:
  ▶ Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.2
  ▶ User Datagram Protocol, Src Port: 41797, Dst Port: 53
  ▶ Domain Name System (query)
```

0000	4a 30 fe 65 8f 13 ba 62	ca b2 e5 d4 08 00 45 00	J0 e... b ... E
0010	00 48 c3 61 00 00 40 11	35 83 c0 a8 00 6e c0 a8	H.a...@. 5 ... n...
0020	00 02 a3 45 00 35 00 34	ab 19 77 b7 00 10 00 01	... E 5 4 ... w...
0030	00 00 00 00 01 03 70	63 32 07 73 74 61 72 74 p c2 start...
0040	75 70 03 6e 65 74 00 00	01 00 01 00 00 29 02 00	up net...)...
0050	00 00 80 00 00 00



step 3 – the sniffer output

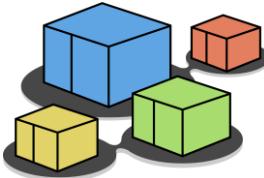
localuni asks dnsstart
what is the address of
pc2.startup.net

	Protocol	Length	Info
10 0.0033...	DNS	75	Standard query 0x7e04 A pc2.startup.net
11 0.0033...	DNS	86	Standard query 0xeabd A pc2.startup.net OPT
12 0.0040...	DNS	70	Standard query 0x3352 NS <Root> OPT
13 0.0049...	DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
14 0.0050...	DNS	110	Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
15 0.0056...	DNS	86	Standard query 0x77b7 A pc2.startup.net OPT
16 0.0060...	DNS	125	Standard query response 0x77b7 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
16 0.0060...	DNS	86	Standard query 0x708f A pc2.startup.net OPT
17 0.0065...	DNS	102	Standard query response 0x708f A pc2.startup.net A 192.168.0.222 OPT
18 0.0072...	DNS	130	Standard query response 0x7e04 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192...
19 0.0076...	DNS	75	Standard query 0x7608 AAAA pc2.startup.net
20 0.0084...	DNS	102	Standard query response 0xffe6 AAAA pc2.startup.net OPT
21 0.0090...	DNS	130	Standard query response 0xffe6 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup.net A 1...
22 0.0093...	DNS	130	Standard query response 0x7608 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup.net A 1...

pc2.startup.net address
is 192.168.0.222

```
Frame 16: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface
Ethernet II, Src: ba:62:ca:b2:e5:d4 (ba:62:ca:b2:e5:d4), Dst: 9e:e8:c9:14:1b:ba (pc2.startup.net)
Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.22
User Datagram Protocol, Src Port: 58066, Dst Port: 53
Domain Name System (query)
```

0000	9e e8 c9 14 67 1b ba 62	ca b2 e5 d4 08 00 45 00	... g . b . . . E
0010	00 48 39 96 00 00 40 11	bf 3a c0 a8 00 6e c0 a8	H9 . @ . : n .
0020	00 16 e2 d2 00 35 00 34	72 a0 70 8f 00 10 00 01 5 . 4 r p . . .
0030	00 00 00 00 01 03 70	63 32 07 73 74 61 72 74 p c2 start
0040	75 70 03 6e 65 74 00 00	01 00 01 00 00 29 02 00	up . net
0050	00 00 80 00 00 00	



step 3 – the sniffer output

localuni reports to pc1 the address of **pc2.startup.net**

No.	Time	Source	Destination	Protocol	Length	Info
0				DNS	75	Standard query 0xb5d4 A pc2.startup.net
1				DNS	86	Standard query 0x8ff1 A pc2.startup.net OPT
2				DNS	70	Standard query 0x7d19 NS <Root> OPT
3				DNS	123	Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
4				DNS	110	Standard query response 0x7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
5				DNS	86	Standard query 0x5ac0 A pc2.startup.net OPT
6				DNS	125	Standard query response 0x5ac0 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
7				DNS	86	Standard query 0x4bba A pc2.startup.net OPT
8				DNS	102	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 OPT
9				DNS	130	Standard query response 0xb5d4 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
10				DNS	75	Standard query 0xeccb AAAA pc2.startup.net
11				DNS	86	Standard query 0x722b AAAA pc2.startup.net OPT
12				DNS	136	Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
13				DNS	125	Standard query response 0xeccb AAAA pc2.startup.net SOA dnsstart.startup.net

Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 1

Queries

Answers

pc2.startup.net: type A, class IN, addr 192.168.0.222

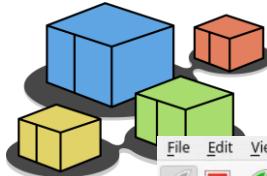
Name: pc2.startup.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 60000 (16 hours, 40 minutes)
Data length: 4
Address: 192.168.0.222

Authoritative nameservers

startup.net: type NS, class IN, ns dnsstart.startup.net

0000 92 93 6c 69 91 fc ee d6 b8 29 cf ae 08 00 45 00 .li....)....E-
0010 00 74 9d 5b 00 00 40 11 5a f0 c0 a8 00 6e c0 a8 .t.[...@. Z....n..
0020 00 6f 00 35 9b 9e 00 60 10 4b b5 d4 81 80 00 01 .o.5...` K....
0030 00 01 00 01 00 01 03 70 63 32 07 73 74 61 72 74p c2.start
0040 75 70 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 up.net...
0050 01 00 00 ea 60 00 04 c0 a8 00 de c0 10 00 02 00`....
0060 01 00 00 ea 60 00 0b 08 64 6e 73 73 74 61 72 74`.... dnsstart
0070 c0 10 c0 3d 00 01 00 01 00 00 ea 60 00 04 c0 a8=....`....
0080 00 16 ..

Packets: 40 · Displayed: 14 (35.0%) · Profile: Default



step 3 – the sniffer output

pc1 asks localuni for AAAA records of pc2.startup.net

localuni directly asks dnsstart (it already knows it) for AAAA records of pc2.startup.net

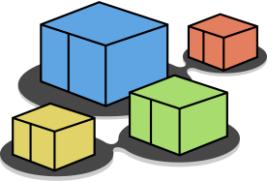
dnsstart returns the AAAA record to localuni

localuni reports dnsstart answer to pc1

The screenshot shows Wireshark capturing DNS traffic between four hosts: pc1 (192.168.0.111), localuni (192.168.0.110), dnsstart (192.168.0.222), and pc2.startup.net (192.168.0.22). The timeline pane shows the sequence of messages:

- Frame 19 (19.0.0076): pc1 queries localuni for AAAA records of pc2.startup.net.
- Frame 20 (19.0.0084): localuni queries dnsstart for AAAA records of pc2.startup.net.
- Frame 21 (19.0.0090): dnsstart responds with the AAAA record for pc2.startup.net.
- Frame 22 (19.0.0093): localuni sends the response back to pc1.

The details pane shows the captured frame data, and the bytes pane shows the raw hex and ASCII representation of the captured data.



step 3 – ping from pc1

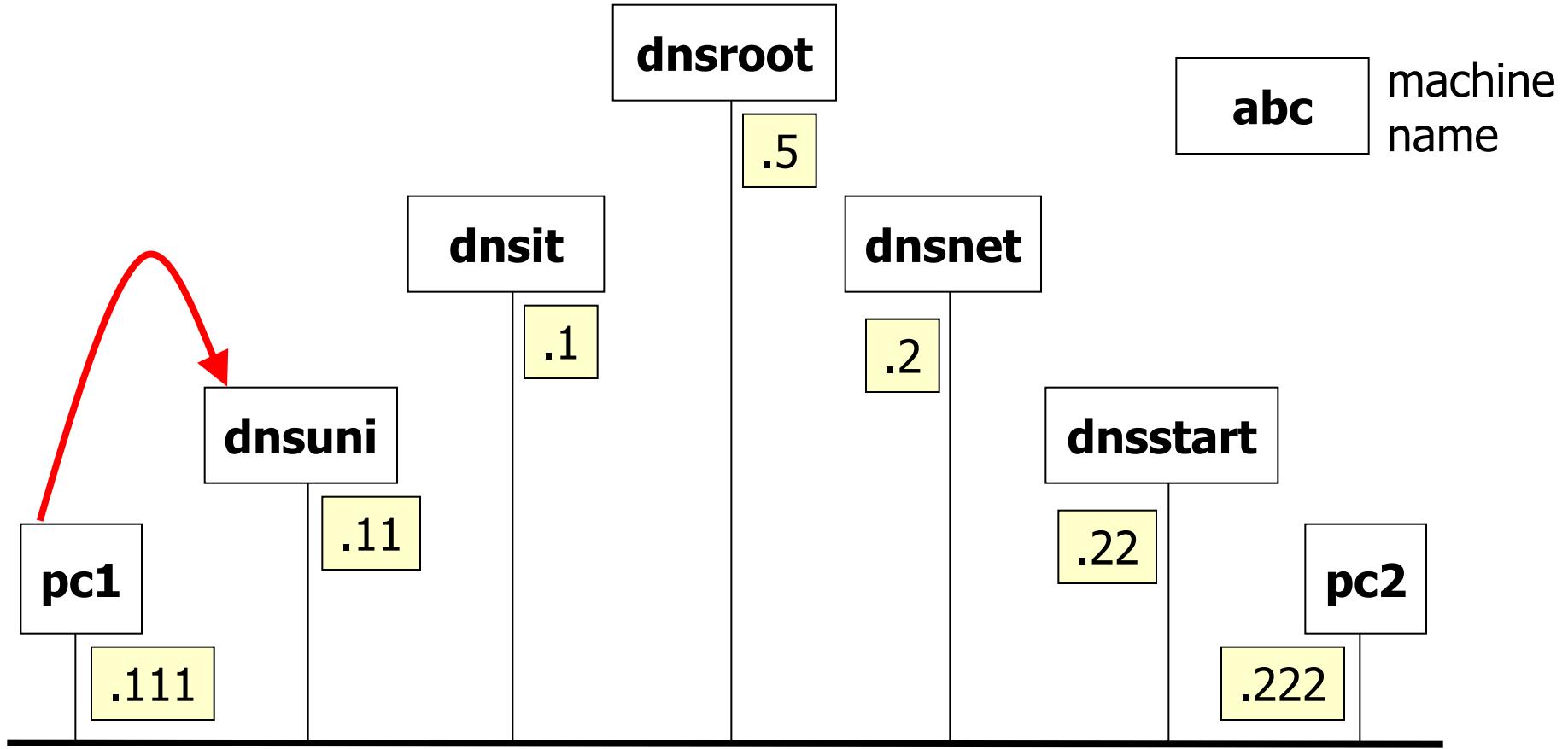
- execute a ping6 command towards pc2

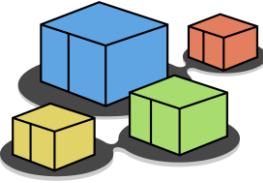
Ping using IPv6 addresses

pc1

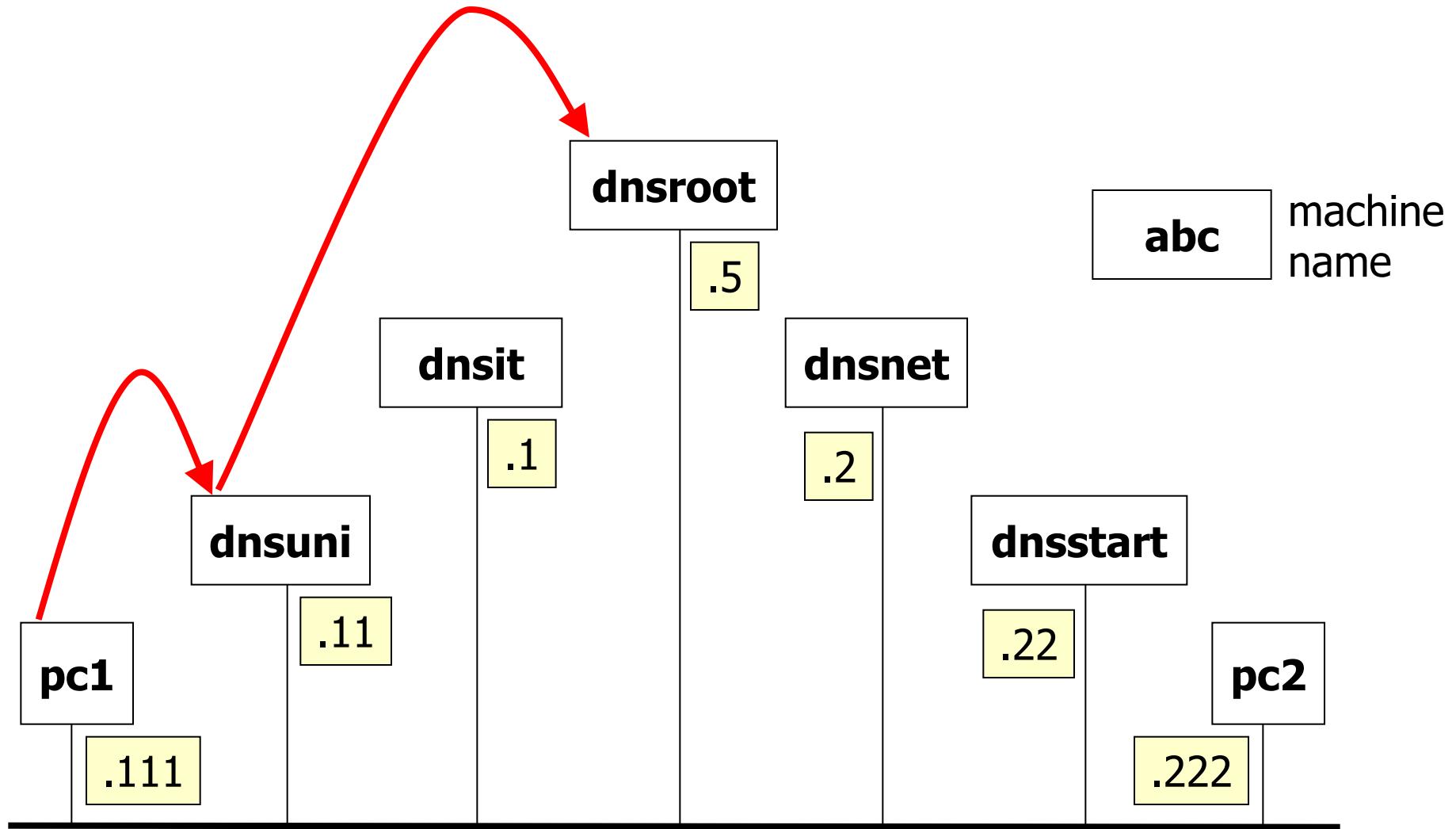
```
root@pc1:/# ping6 -n pc2.startup.net
PING pc2.startup.net(2001:a::2) 56 data bytes
64 bytes from 2001:a::2: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 2001:a::2: icmp_seq=2 ttl=64 time=0.696 ms
64 bytes from 2001:a::2: icmp_seq=3 ttl=64 time=0.686 ms
64 bytes from 2001:a::2: icmp_seq=4 ttl=64 time=0.974 ms
--- pc2.startup.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3303ms
rtt min/avg/max/mdev = 0.686/0.844/1.020/0.153 ms
```

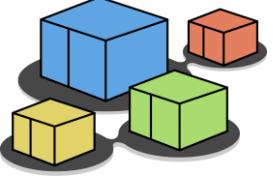
step 3 – exchanged messages



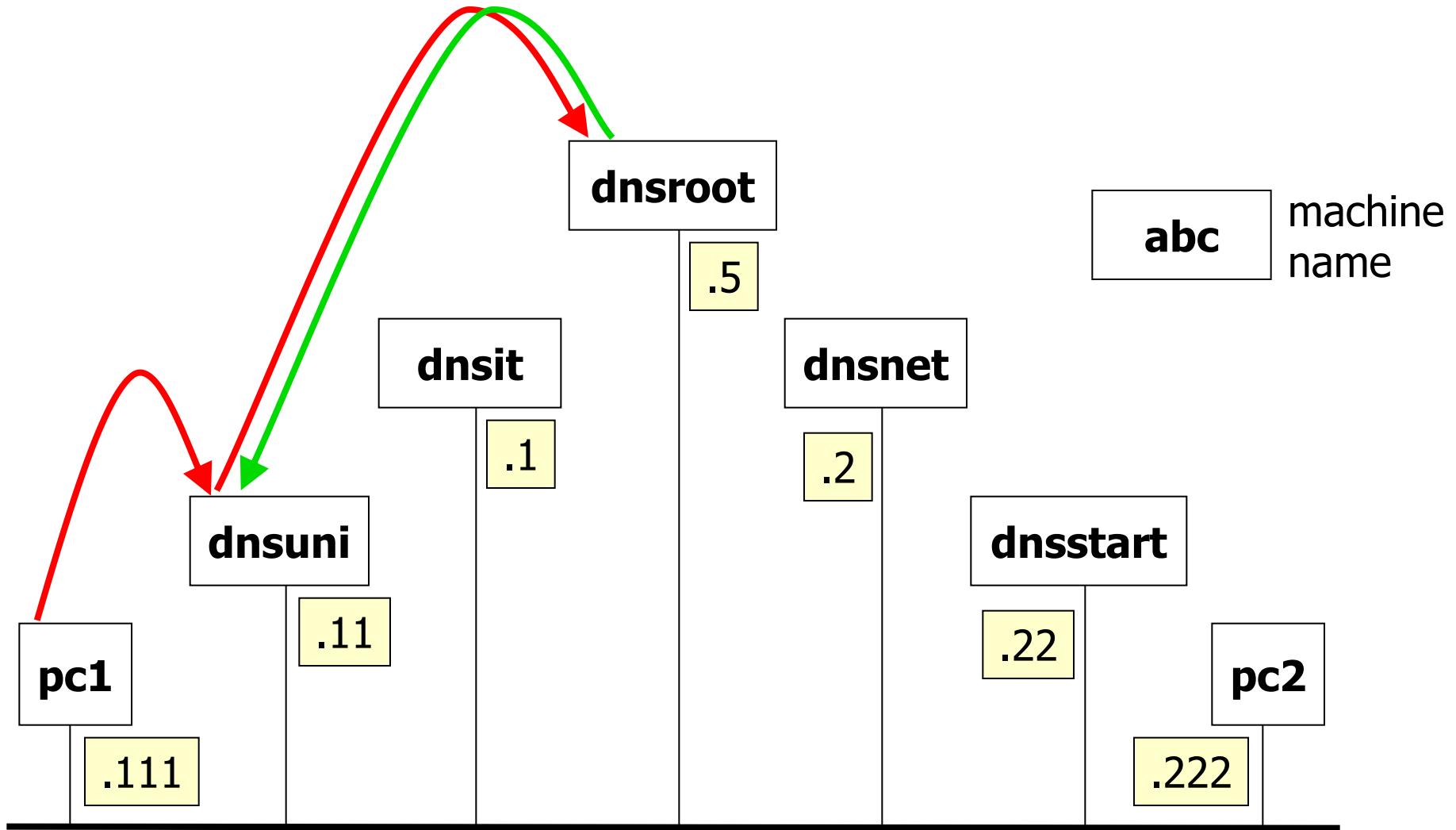


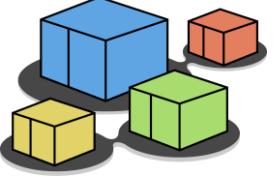
step 3 – exchanged messages



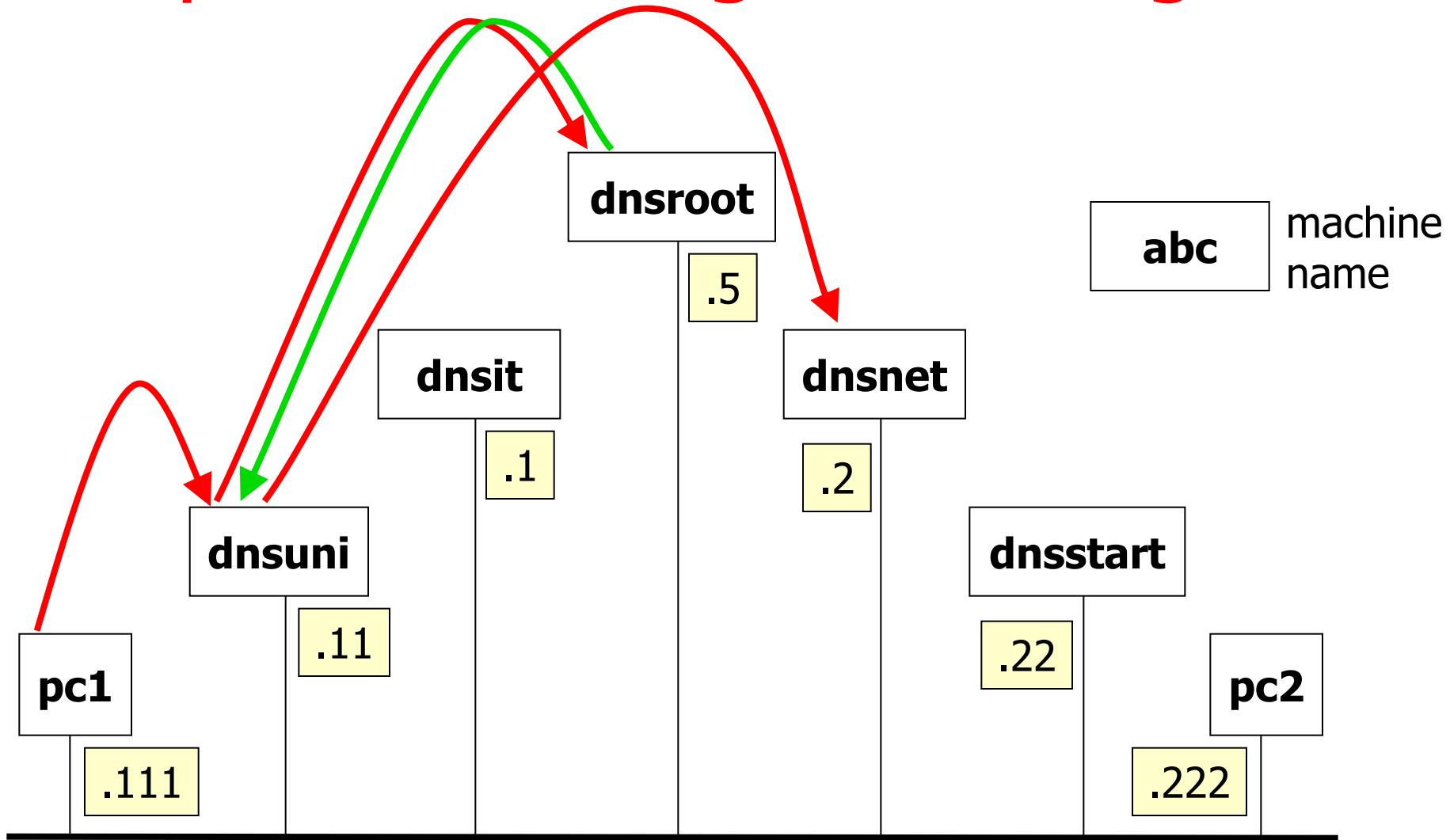


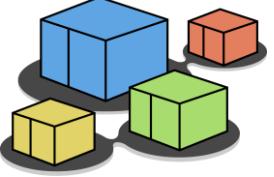
step 3 – exchanged messages



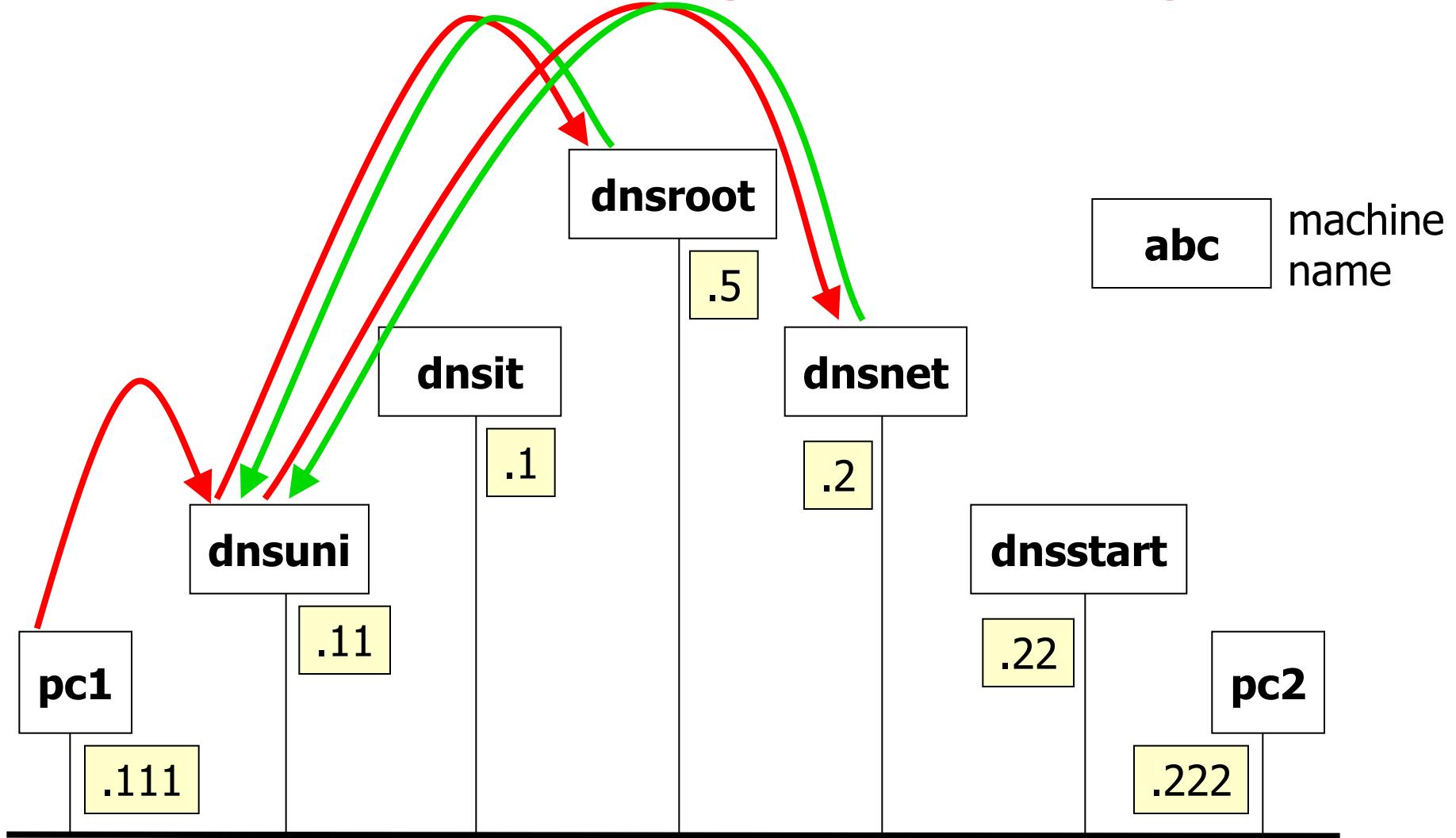


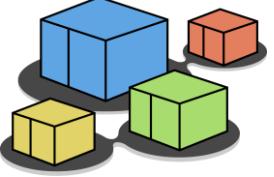
step 3 – exchanged messages



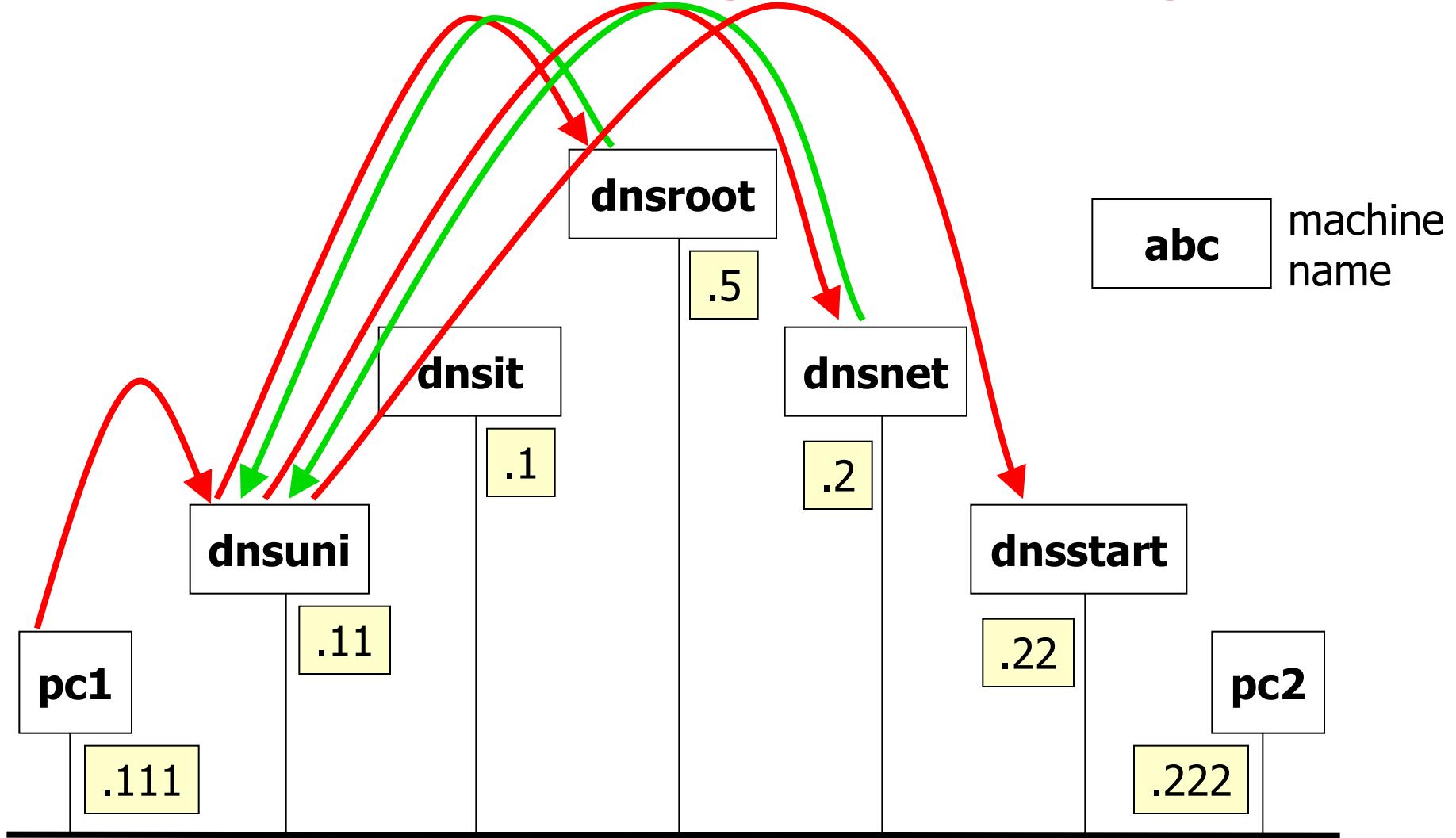


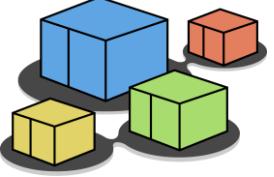
step 3 – exchanged messages



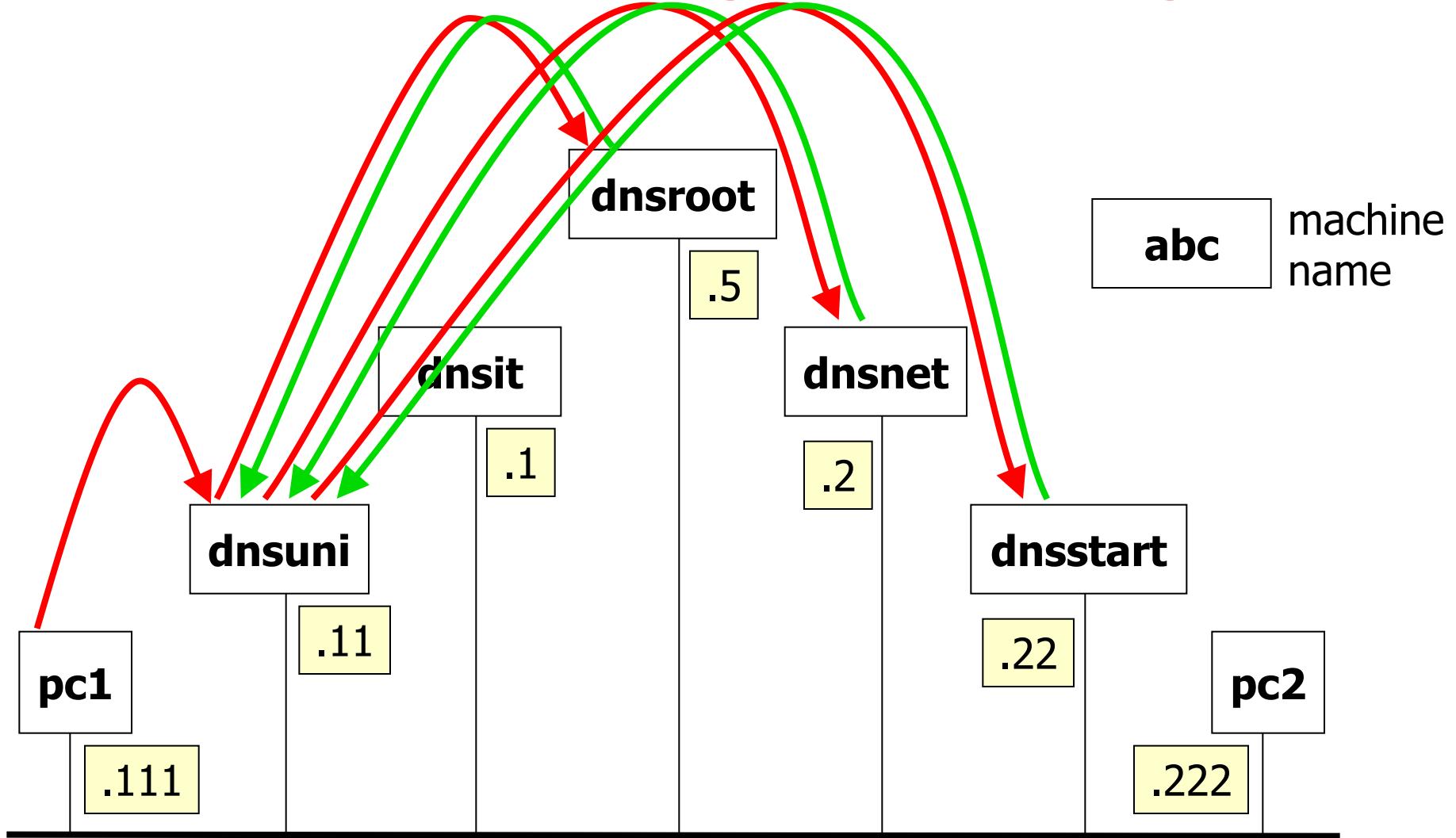


step 3 – exchanged messages



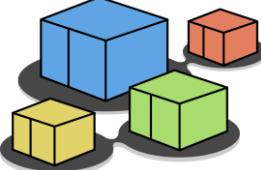


step 3 – exchanged messages

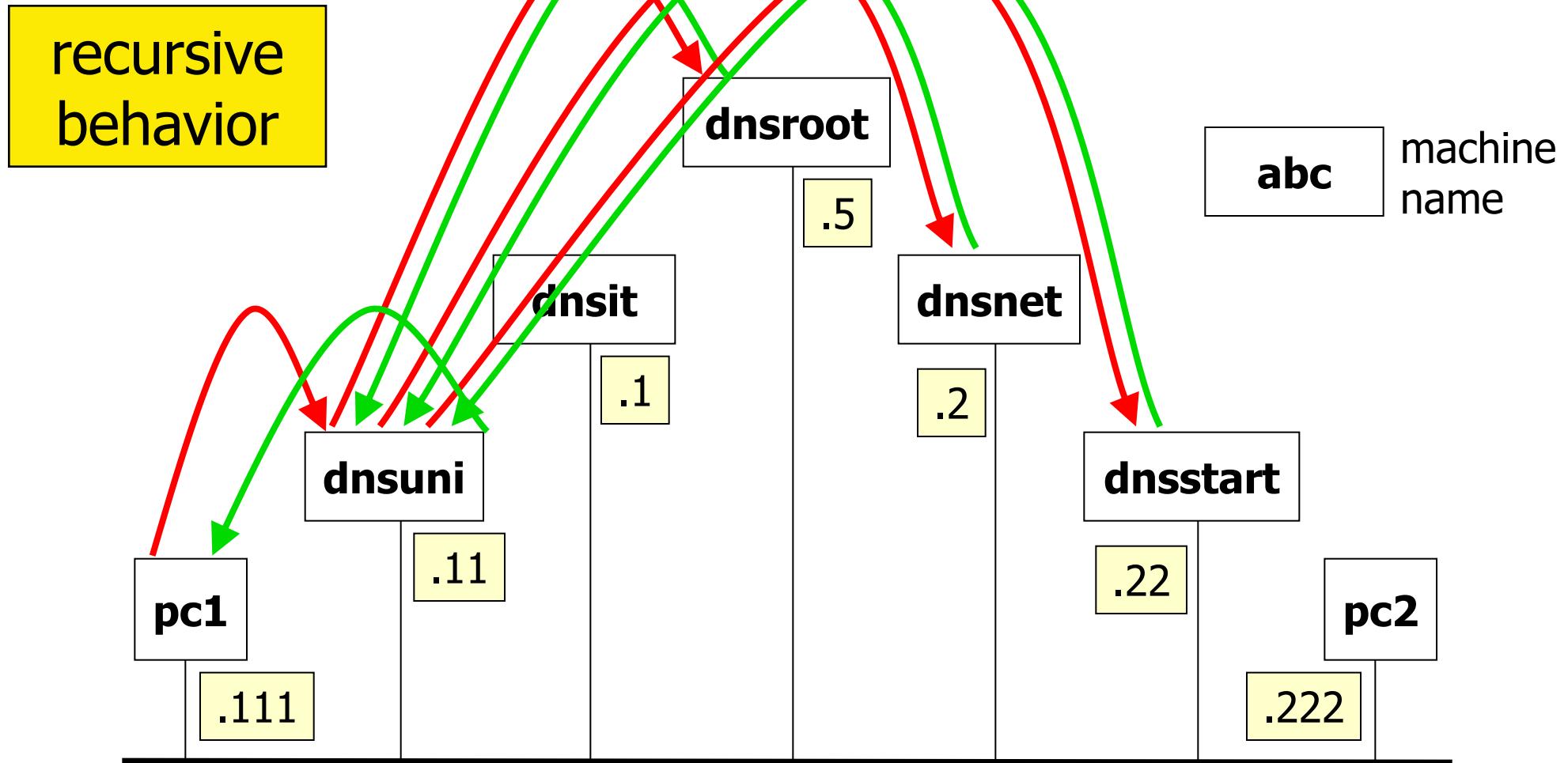


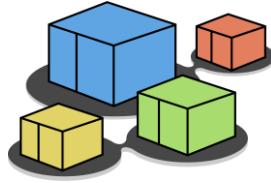
192.168.0.0/24

kathara – [lab: dns]



step 3 – exchanged messages

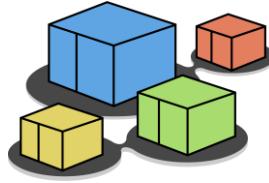




step 4 – repeating the experiment

- execute a ping command towards pc2

```
pc1
root@pc1:/# ping -n pc2.startup.net
PING pc2.startup.net (192.168.0.222) 56(84) bytes of data.
64 bytes from 192.168.0.222: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 192.168.0.222: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.0.222: icmp_seq=3 ttl=64 time=0.525 ms
--- pc2.startup.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.525/0.867/1.496/0.445 ms
```



step 4 – repeating the experiment

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.0.111	192.168.0.110	DNS	75 Standard query 0x591b A pc2.startup.net
2	0.001971994	192.168.0.110	192.168.0.111	DNS	130 Standard query response 0x591b A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
3	0.002335337	192.168.0.111	192.168.0.110	DNS	75 Standard query 0x9e05 AAAA pc2.startup.net
4	0.002768557	192.168.0.110	192.168.0.111	DNS	125 Standard query response 0x9e05 AAAA pc2.startup.net SOA dnsstart.startup.net

the name server cache helps reducing traffic

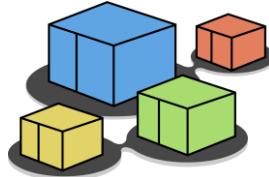
Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth0
Ethernet II, Src: 92:93:6c:69:91:fc (92:93:6c:69:91:fc), Dst: ee:d6:b8:29:cf:ae (ee:d6:b8:29:cf:ae)
Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110
User Datagram Protocol, Src Port: 35784, Dst Port: 53
Domain Name System (query)
 Transaction ID: 0x591b
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 [Response In: 21](#)

0000	ee d6 b8 29 cf ae 92 93 6c 69 91 fc 08 00 45 00	...).... li....E-
0010	00 3d c8 0e 40 00 40 11 f0 73 c0 a8 00 6f c0 a8	=...@... s...o...
0020	00 6e 8b c8 00 35 00 29 62 16 59 1b 01 00 00 01	n...5...) b.Y....
0030	00 00 00 00 00 00 03 70 63 32 07 73 74 61 72 74p c2 start
0040	75 70 03 6e 65 74 00 00 01 00 01	up.net....

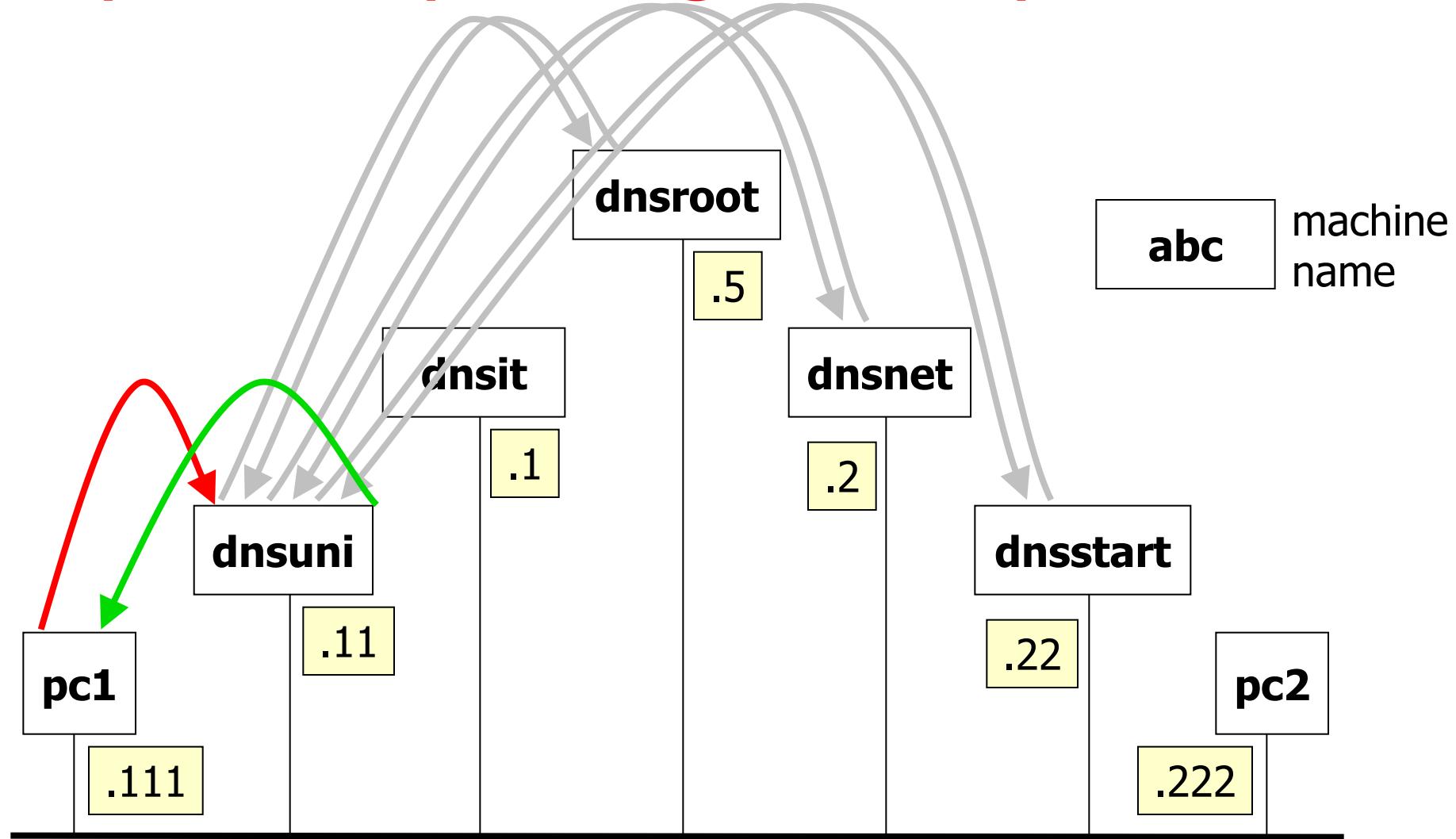
eth1: <live capture in progress>

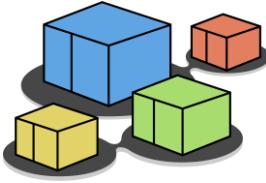
Packets: 16 · Displayed: 4 (25.0%)

Profile: Default



step 4 – repeating the experiment

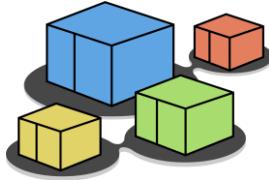




step 5 – cleaning the cache

```
localuni
root@localuni:/# rndc flush
```

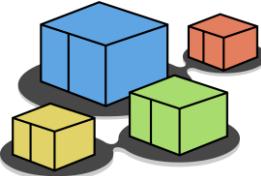
- rndc controls the operation of a name server
- the flush command cleans up caches
 - a new client query triggers the complete sequence of iterative queries



step 6 – ping non-existent target

- execute a ping command towards a non-existent target

```
pc1
root@pc1:/# ping pluto.startup.net
ping: pluto.startup.net: Name or service not known
```



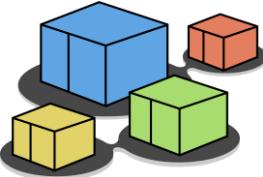
step 6 – non-existent target

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.0...	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x5ca4 A pluto.startup.net
2	0.0...	192.168.0.110	192.168.0.5	DNS	88	Standard query 0x2cb4 A pluto.startup.net OPT
3	0.0...	192.168.0.110	192.168.0.5	DNS	70	Standard query 0xd75d NS <Root> OPT
4	0.0...	192.168.0.5	192.168.0.110	DNS	125	Standard query response 0x2cb4 A pluto.startup.net NS dnsnet.net A 192.168.0.2 OPT
5	0.0...	192.168.0.110	192.168.0.2	DNS	88	Standard query 0x6ee4 A pluto.startup.net OPT
6	0.0...	192.168.0.5	192.168.0.110	DNS	110	Standard query response 0xd75d NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
7	0.0...	192.168.0.2	192.168.0.110	DNS	127	Standard query response 0x6ee4 A pluto.startup.net NS dnsstart.startup.net A 192.168.0.22 ...
8	0.0...	192.168.0.110	192.168.0.110	DNS	88	Standard query 0xbe7c A pluto.startup.net OPT
9	0.0...	192.168.0.22	192.168.0.110	DNS	138	Standard query response 0xbe7c No such name A pluto.startup.net SOA dnsstart.startup.net 0...
→ 10	0.0...	192.168.0.110	192.168.0.111	DNS	77	Standard query response 0x5ca4 No such name A pluto.startup.net SOA dnsstart.startup.net
11	0.0...	192.168.0.111	192.168.0.110	DNS	64	Standard query 0xb4a0 AAAA pluto.startup.net
12	0.0...	192.168.0.110	192.168.0.111	DNS	64	Standard query response 0xb4a0 No such name AAAA pluto.startup.net SOA dnsstart.startup.net

all the iterative queries are performed again because of the cache flush

Frame 1: 77 bytes on wire (616 bits)
Ethernet II, Src: f2:84:08:67:54:30, Dst: 00:0c:29:1e:00:00
Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110
User Datagram Protocol, Src Port: 49152, Dst Port: 53
Domain Name System (query)
 Transaction ID: 0x5ca4
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 [Response In: 10]

b2 e5 d4 f2 84 08 67 54 3c 08 00 45 00 b.....g
45 40 00 40 11 dc 3a c0 a8 00 6f c0 a8 ?E@...:
e3 00 35 00 2b c2 bb 5c a4 01 00 00 01 n...5+...
00 00 00 05 70 6c 75 74 6f 07 73 74 61p lu
5 70 03 6e 65 74 00 00 01 00 01 rtup.net ..



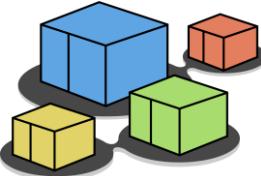
step 6 – non-existent target

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.0...	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x5ca4 A pluto.startup.net
2	0.0...	192.168.0.110	192.168.0.5	DNS	88	Standard query 0x2cb4 A pluto.startup.net OPT
3	0.0...	192.168.0.110	192.168.0.5	DNS	70	Standard query 0xd75d NS <Root> OPT
4	0.0...	192.168.0.5	192.168.0.110	DNS	125	Standard query response 0x2cb4 A pluto.startup.net NS dnsnet.net A 192.168.0.2 OPT
5	0.0...	192.168.0.110	192.168.0.2	DNS	88	Standard query 0x6ee4 A pluto.startup.net OPT
6	0.0...	192.168.0.5	192.168.0.110	DNS	110	Standard query response 0xd75d NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
7	0.0...	192.168.0.2	192.168.0.110	DNS	127	Standard query response 0x6ee4 A pluto.startup.net NS dnsstart.startup.net A 192.168.0.22 ...
8	0.0...	192.168.0.110	192.168.0.22	DNS	88	Standard query 0xbe7c A pluto.startup.net OPT
9	0.0...	192.168.0.22	192.168.0.110	DNS	138	Standard query response 0xbe7c No such name A pluto.startup.net SOA dnsstart.startup.net 0...
→ 10	0.0...	192.168.0.110	192.168.0.111	DNS	127	Standard query response 0x5ca4 No such name A pluto.startup.net SOA dnsstart.startup.net
11	0.0...	192.168.0.111	192.168.0.110	DNS	77	Standard query 0xb4a0 AAAA pluto.startup.net
12	0.0...	192.168.0.110	192.168.0.111	DNS	127	Standard query response 0xb4a0 No such name AAAA pluto.startup.net SOA dnsstart.startup.net

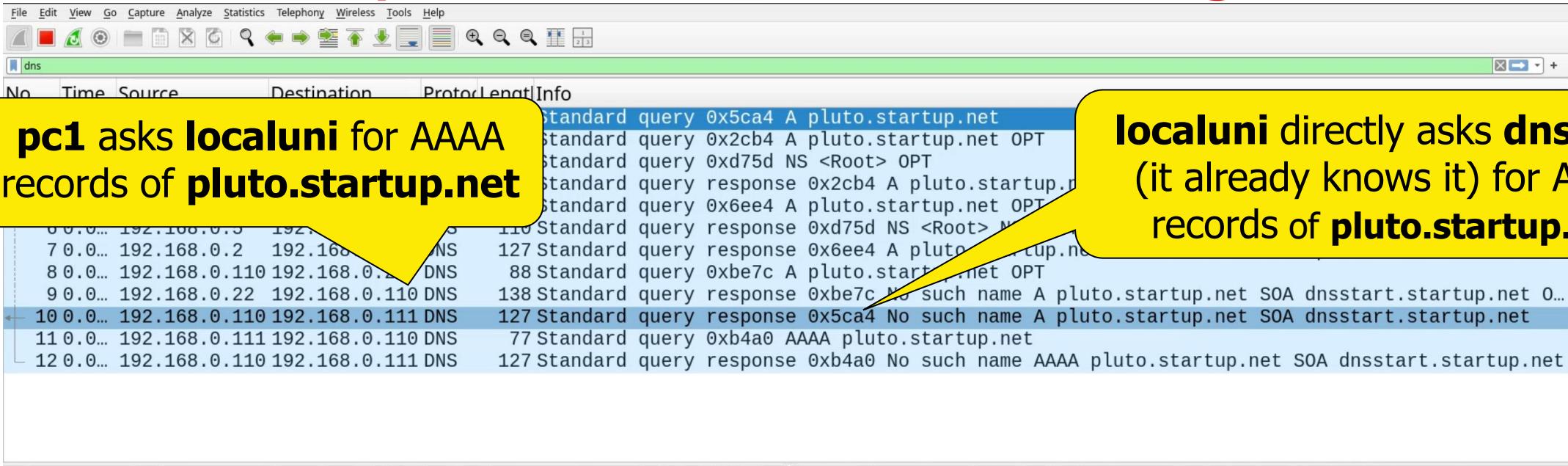
```
› Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
› Ethernet II, Src: f2:84:08:67:54:3c (f2:84:08:67:54:3c), Dst: ba...
› Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110
› User Datagram Protocol, Src Port: 42979, Dst Port: 53
› Domain Name System (query)
  Transaction ID: 0x5ca4
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
› Queries
  [Response In: 10]
```

the requested domain
(pluto.startup.net)
does not exist

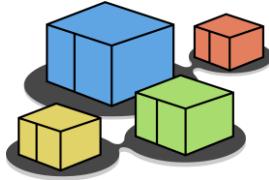
```
8 00 45 00 .b....g
0 6f c0 a8 .?E@.:@:
1 00 00 01 .n...5+...
7 73 74 61 .....p lu
1 rtp.net ..
```



step 6 – non-existent target

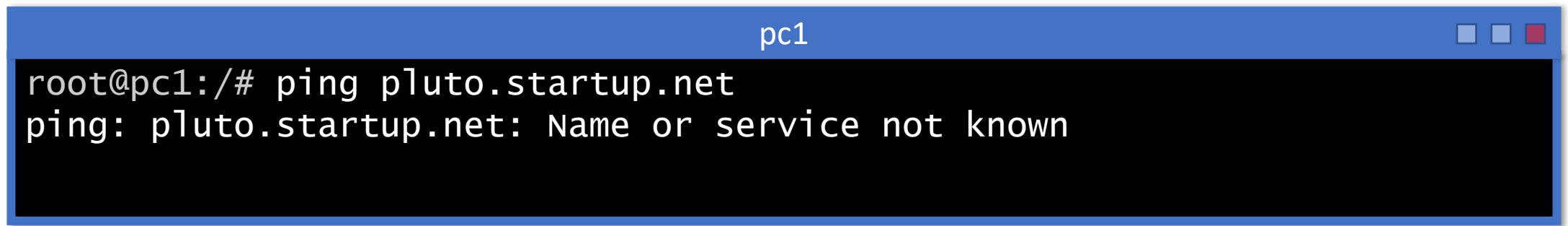


0000	ba	62	ca	b2	e5	d4	f2	84	08	67	54	3c	08	00	45	00	.b.....g
0010	00	3f	dc	45	40	00	40	11	dc	3a	c0	a8	00	6f	c0	a8	.?·E@·@..:
0020	00	6e	a7	e3	00	35	00	2b	c2	bb	5c	a4	01	00	00	01	.n...5+..
0030	00	00	00	00	00	00	05	70	6c	75	74	6f	07	73	74	61·p lu
0040	72	74	75	70	03	6e	65	74	00	00	01	00	01	rtp	.net ..		

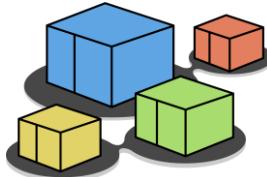


step 6 – ping non-existent target

- repeat the ping command towards the non-existent target



```
pc1
root@pc1:/# ping pluto.startup.net
ping: pluto.startup.net: Name or service not known
```



step 6 – ping non-existent target

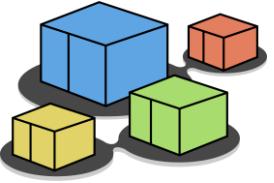
the name server negative cache has stored the negative answer

No.	Source	Destination	Protocol	Length	Info
1	0.0.0.0	192.168.0.110	DNS	77	Standard query A pluto.startup.net
2	0.0.0.0	192.168.0.110	DNS	127	Standard query response 0xeb70 No such name A pluto.startup.net SOA dnsstart.startup.net
3	0.0.0.1	192.168.0.110	DNS	77	Standard query 0xeb07 AAAA pluto.startup.net
4	0.0.0.1	192.168.0.110	DNS	127	Standard query response 0xeb07 No such name AAAA pluto.startup.net SOA dnsstart.startup.net

Frame 2: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits)
Ethernet II, Src: da:e3:47:a3:3c:22 (da:e3:47:a3:3c:22), Dst: 8e:e3:
Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.111
User Datagram Protocol, Src Port: 53, Dst Port: 33575
Domain Name System (response)
Transaction ID: 0xeb70
Flags: 0x8183 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
[\[Request In: 1\]](#)
[Time: 0.000804085 seconds]

0000	8e e3 c4 b3 07 17 da e3 47 a3 3c 22 08 00 45 00 G
0010	00 71 3a ea 00 00 40 11 bd 64 c0 a8 00 6e c0 a8	q:...@.. d ..
0020	00 6f 00 35 83 27 00 5d 44 25 eb 70 81 83 00 01	o 5.'] D%
0030	00 00 00 01 00 00 05 70 6c 75 74 6f 07 73 74 61	p lu
0040	72 74 75 70 03 6e 65 74 00 00 01 00 01 c0 12 00	rtp.net
0050	06 00 01 00 00 28 a4 00 26 08 64 6e 73 73 74 61	(... & ..
0060	72 74 c0 12 04 72 6f 6f 74 c0 2f 78 a5 a0 51 00	rt...roo t ..
0070	00 00 1c 00 00 38 40 00 36 ee 80 00 00 00 0f8@.. 6 ..

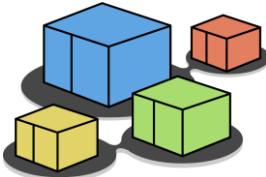
Packets: 8 · Displayed: 4 (50.0%) Profile: Default



step 7 – advanced queries

- resource records can be searched by using **dig**
 - highly customizable queries
 - detailed responses

```
pc1
root@pc1:/# dig pc2.startup.net
```



step 7 – advanced queries

pc1

Request ANY type of record

```
root@pc1:/# dig ANY pc2.startup.net
...
<>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

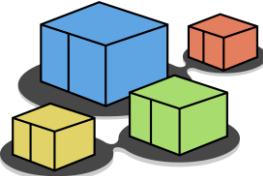
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA    2001:a::2
pc2.startup.net. 59985    IN      A       192.168.0.222

;; AUTHORITY SECTION:
startup.net.      59985    IN      NS      dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59985    IN      A       192.168.0.22

;; Query time: 0 msec
```



step 7 – advanced queries

answer flags:
qr: query response
rd: recursion desired (the user asked for a recursive lookup)
ra: recursion available (the server allows recursive lookups)

pc1

```
root@pc1:/# dig ANY pc2.startup.net

; <>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

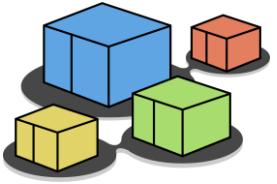
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA    2001:a::2
pc2.startup.net. 59985    IN      A       192.168.0.222

;; AUTHORITY SECTION:
startup.net.      59985    IN      NS      dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59985    IN      A       192.168.0.22

;; Query time: 0 msec
```



step 7 – advanced queries

pc1

```
root@pc1:/# dig ANY pc2.startup.net

; <>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

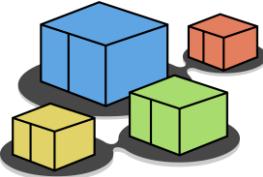
;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA     2001:a::2
pc2.startup.net. 59985    IN      A        192.168.0.222

;; AUTHORITY SECTION:
startup.net.      59985    IN      NS       dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59985    IN      A        192.168.0.22

;; Query time: 0 msec
```

these sections
correspond to those
contained in DNS
packets



step 7 – advanced queries

records being searched
(class: **IN**, type: **ANY** ⇒
IPv4 and IPv6 address
records)

a dns message never
contains more than one
question section

```
pc1
root@pc1:/# dig ANY pc2.startup.net

; <>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

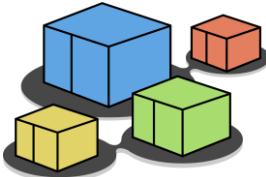
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA    2001:a::2
pc2.startup.net. 59985    IN      A       192.168.0.222

;; AUTHORITY SECTION:
startup.net.      59985    IN      NS      dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59985    IN      A       192.168.0.22

;; Query time: 0 msec
```



step 7 – advanced queries

records that form the answer to the question may be more than one

pc1

```
root@pc1:/# dig ANY pc2.startup.net

; <>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

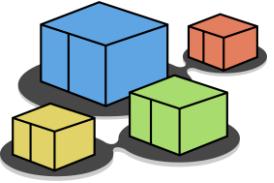
;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA    2001:a::2
pc2.startup.net. 59985    IN      A       192.168.0.222
```

time to live of a resource record that is cached on the server

- try invoking `dig` once more to see it decreasing
- constant if the record is not cached (i.e., it is stored on the name server being queried – by default the one configured in `/etc/resolv.conf`)

NS dnsstart.startup.net.

IN A 192.168.0.22



step 7 – advanced queries

pc1

```
root@pc1:/# dig ANY pc2.startup.net

; <>> DiG 9.18.33-1~deb12u2-Debian <>> ANY pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44527
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 687ce57b4ac279a3f4e52ff069370cf138b6fc2d8a7548a1 (good)
;; QUESTION SECTION:
;pc2.startup.net.      IN      ANY

;; ANSWER SECTION:
pc2.startup.net. 59985    IN      AAAA    2001:a::2
pc2.startup.net. 59985    IN      A       192.168.0.222

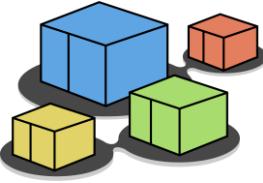
;; AUTHORITY SECTION:
startup.net.      59985    IN      NS      dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59985    IN      A       192.168.0.22

;; Query time: 0 msec
```

records describing authoritative name servers are returned here

additional records are returned here



step 8 – an iterative query

- restart bind on the name server

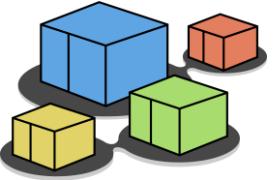
```
localuni
root@localuni:/# systemctl restart bind9
```

- perform an iterative query using **dig**

```
pc1
root@pc1:/# dig +noquestion +noadditional +norecurse pc2.startup.net
```

avoid displaying question
and additional sections

disable recursion



step 8 – an iterative query

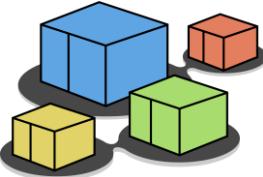
the server answers by specifying the authoritative name server to be contacted to get the desired information

```
pc1
root@pc1:/# dig +noquestion +noadditional +norecurse pc2.startup.net

; <>> DiG 9.18.19-1~deb12u1-Debian <>> +noquestion +noadditional
+norecurse pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15543
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5ea4ced6cdaf30599571a9e0657b15c2381005312bcc21e9 (good)
;; AUTHORITY SECTION:
.                      0           IN         NS        ROOT-SERVER.

;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:48:34 UTC 2023
;; MSG SIZE  rcvd: 96
```



step 8 – an iterative query

query a specific name
server (**dnsroot**)

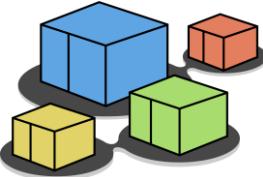
dnsnet.net is the
authoritative name
server for zone **net**

```
pc1
root@pc1:/# dig +noquestion +noadditional +norecurse @192.168.0.5 pc2.startup.net

;   version: 9.18.19-1~deb12u1-Debian <>> +noquestion +noadditional +norecurse
@192.168.0.5 pc2.startup.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24163
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 301c8e7f8267ad01ed2cc63e657b1736676e072f5ecd90bf (good)
;; AUTHORITY SECTION:
net.          60000    IN      NS      dnsnet.net.

;; Query time: 0 msec
;; SERVER: 192.168.0.5#53(192.168.0.5) (UDP)
;; WHEN: Thu Dec 14 14:54:46 UTC 2023
;; MSG SIZE  rcvd: 109
```



step 8 – an iterative query

query a specific name server (**dnsnet.net**)

dnsstart.startup.net
is the authoritative
name server for zone
startup.net

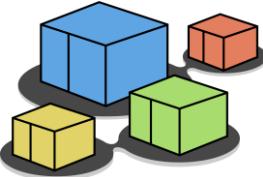
pc1

```
root@pc1:/# dig +noquestion +noadditional +norecurse @192.168.0.2 pc2.startup.net

; <>> DiG 9.18.10.1 +noquestion +noadditional +norecurse
@192.168.0.2 pc2.startup.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42339
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: d96ea5b92e6860aeed2cc63e657b1878e06d204302aa8149 (good)
;; AUTHORITY SECTION:
startup.net.          60000   IN      NS      dnsstart.startup.net.

;; Query time: 9 msec
;; SERVER: 192.168.0.2#53(192.168.0.2) (UDP)
;; WHEN: Thu Dec 14 15:00:08 UTC 2023
;; MSG SIZE  rcvd: 111
```



step 8 – an iterative query

query a specific name
server:
dnsstart.startup.net

the address of
pc2.startup.net

```
pc1
root@pc1:/# dig +noquestion +noadditional +norecurse @192.168.0.22 pc2.startup.net

; <>> DiG 9.18.19-1~deb12u1-1+deb12.1+dfsg-1.2023.12.14.14.56+0.000s <>> +noquestion +noadditional +norecurse
@192.168.0.22 pc2.startup.net
...
global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49113
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: b119e8f8b644792eb3bafbd6657b17989cd95e340adb2072 (good)
;; ANSWER SECTION:
pc2.startup.net.      60000    IN      A      192.168.0.222
;;
;; AUTHORITY SECTION:
startup.net.          60000    IN      NS     dnsstart.startup.net.
;;
;; Query time: 0 msec
;; SERVER: 192.168.0.22#53(192.168.0.22) (UDP)
;; WHEN: Thu Dec 14 14:56:24 UTC 2023
;; MSG SIZE  rcvd: 127
```