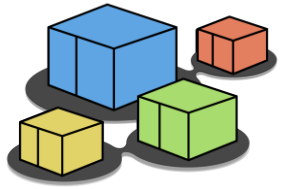
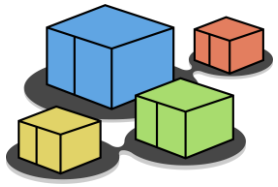


Kathará

kathara lab

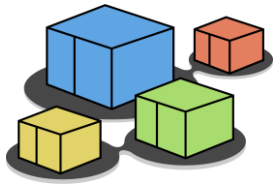
DNS

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



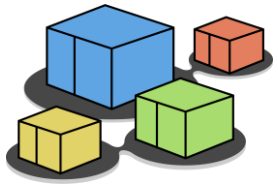
copyright notice

- 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.



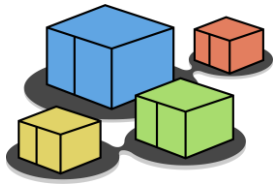
purpose of this lab

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



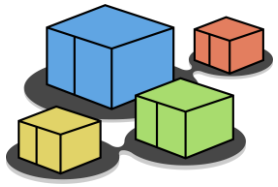
lab limitations

- 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



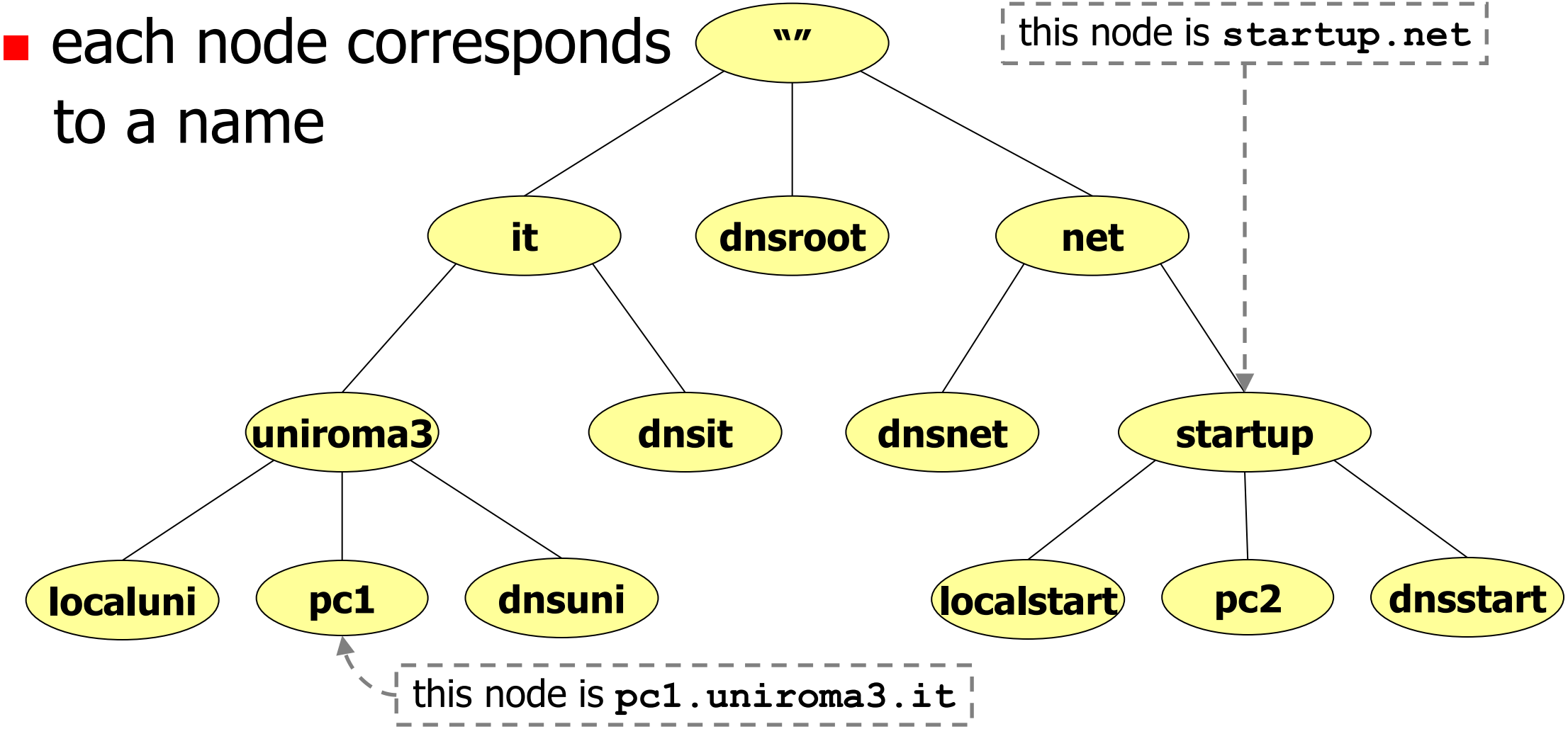
about the DNS

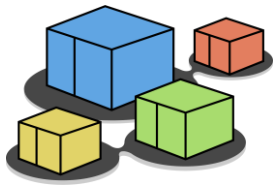
- takes care of associating names with IP addresses
- the name system is distributed over several nodes (hosts) that are hierarchically organized to form a tree
- each node in the hierarchy corresponds to a name
- a domain in the name system is a subtree
- a node in the hierarchy may be delegated to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

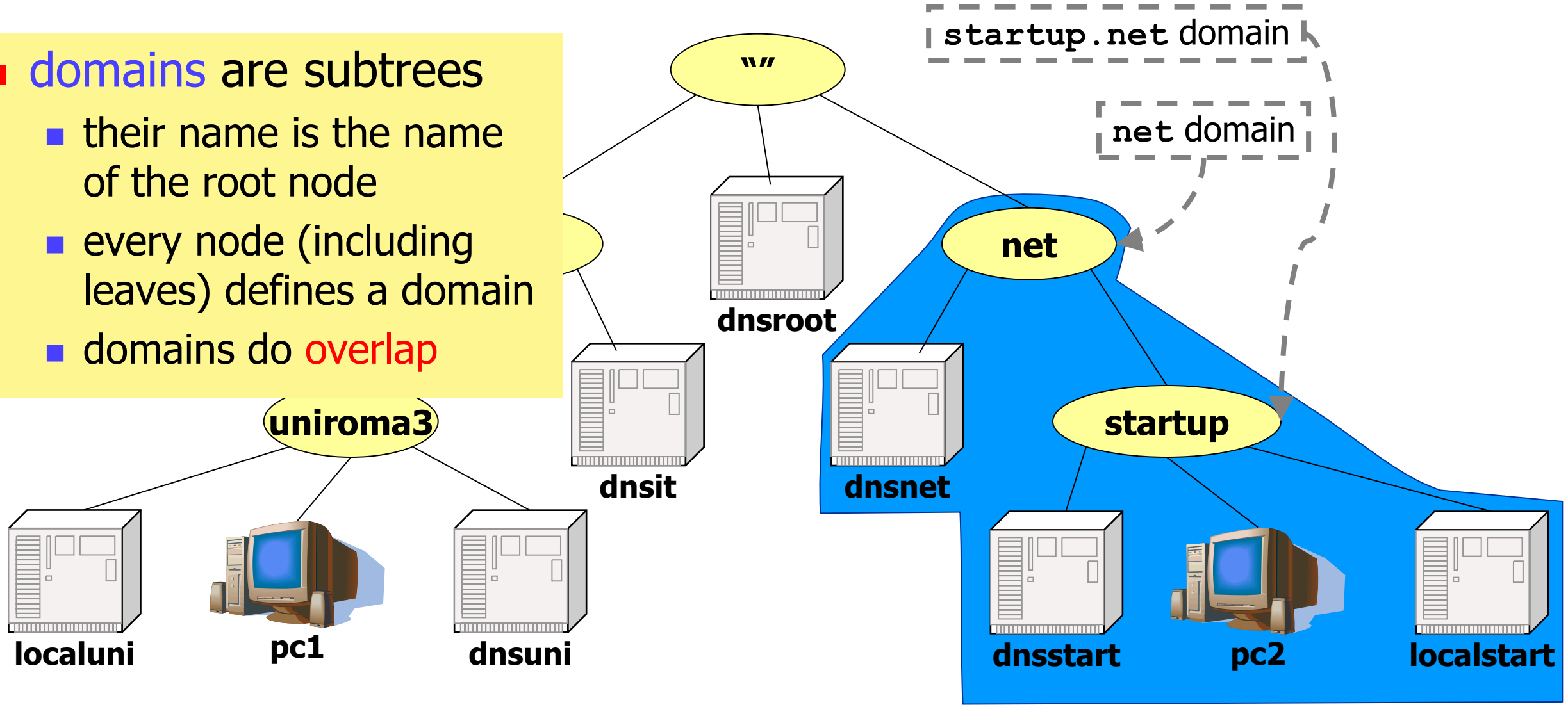
- each node corresponds to a name

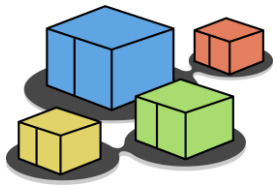




the DNS name hierarchy

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

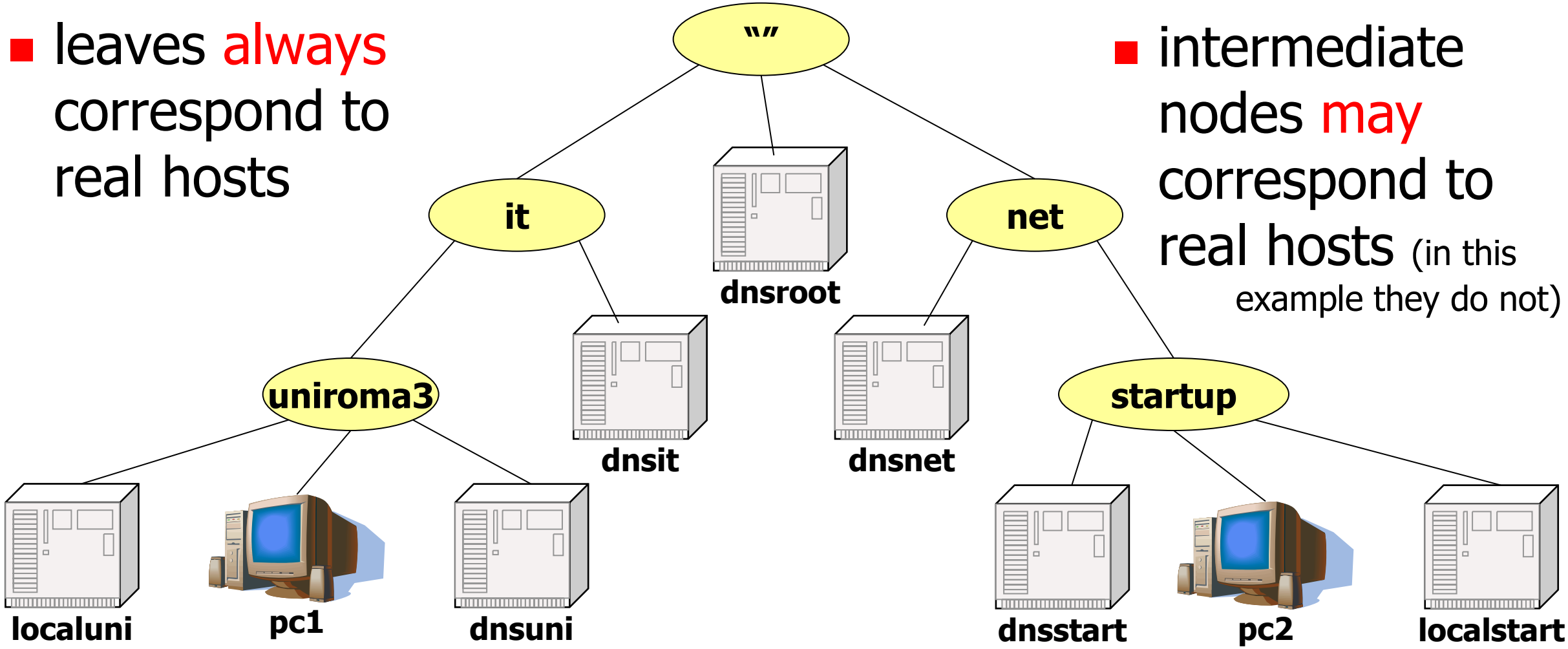


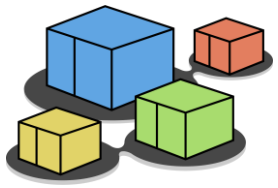


the DNS name hierarchy

- leaves always correspond to real hosts

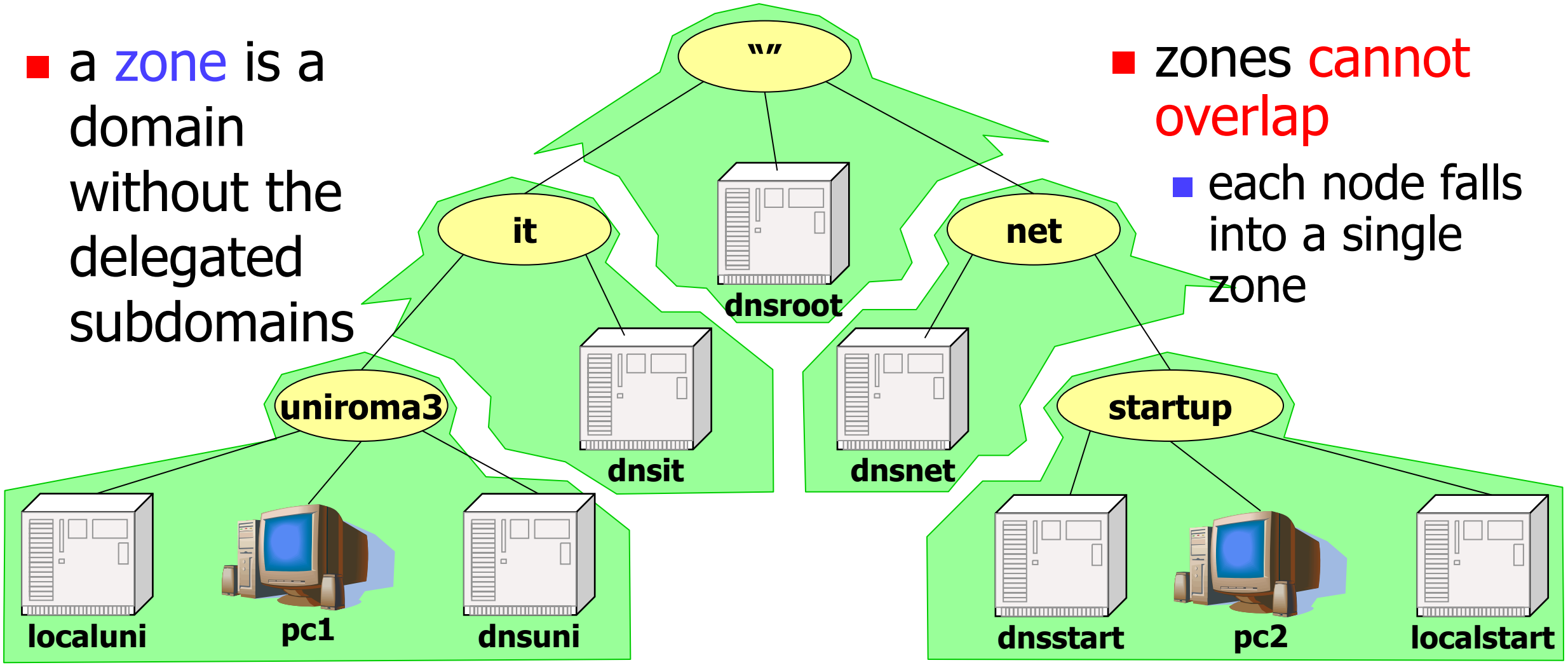
- intermediate nodes may correspond to real hosts (in this example they do not)



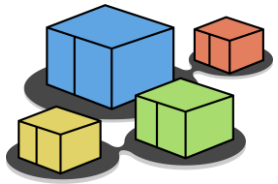


zones

- a zone is a domain without the delegated subdomains

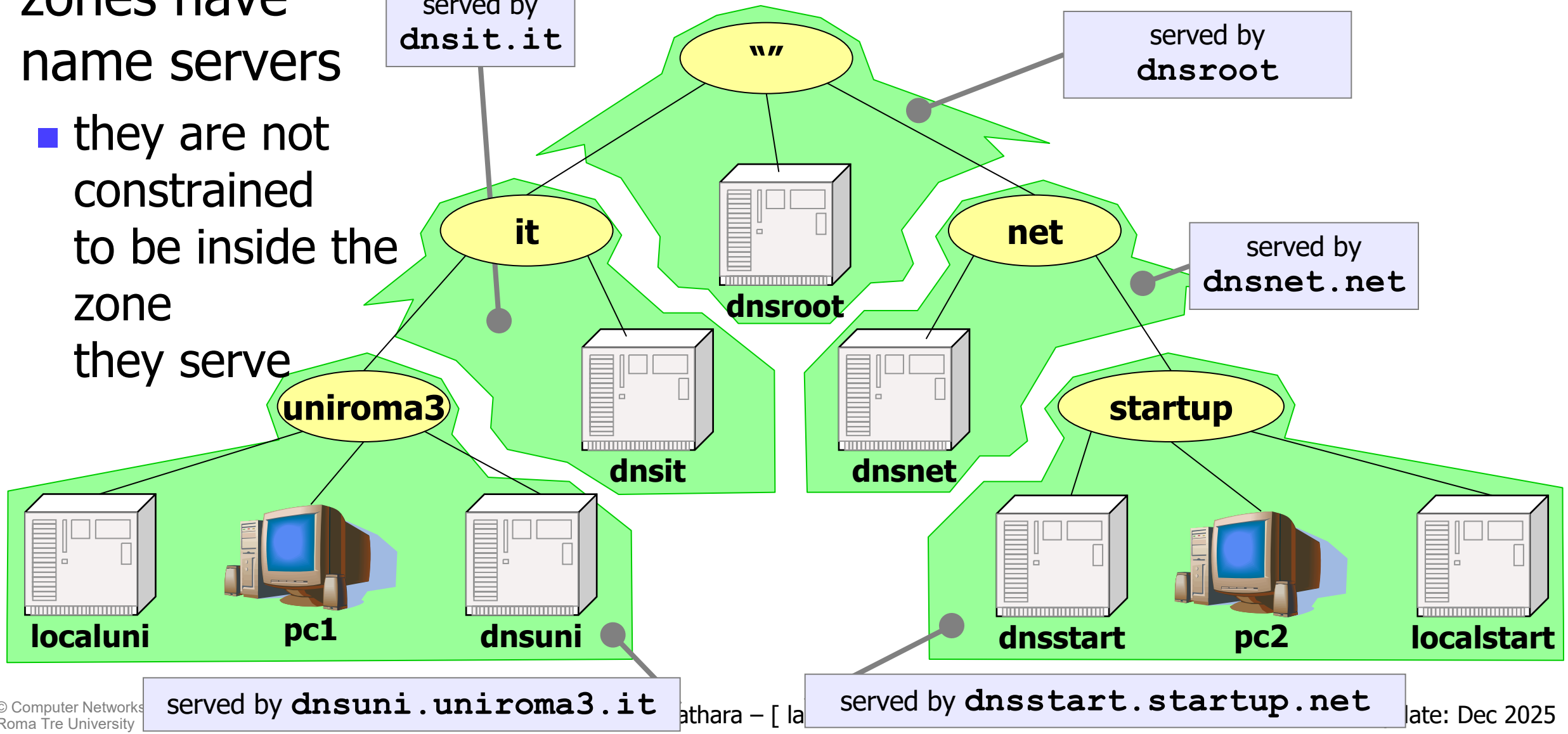


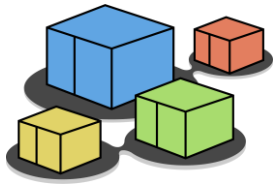
- zones cannot overlap
  - each node falls into a single zone



zones

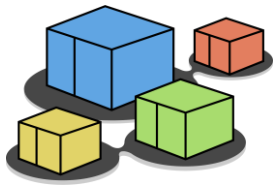
- zones have name servers
  - they are not constrained to be inside the zone they serve



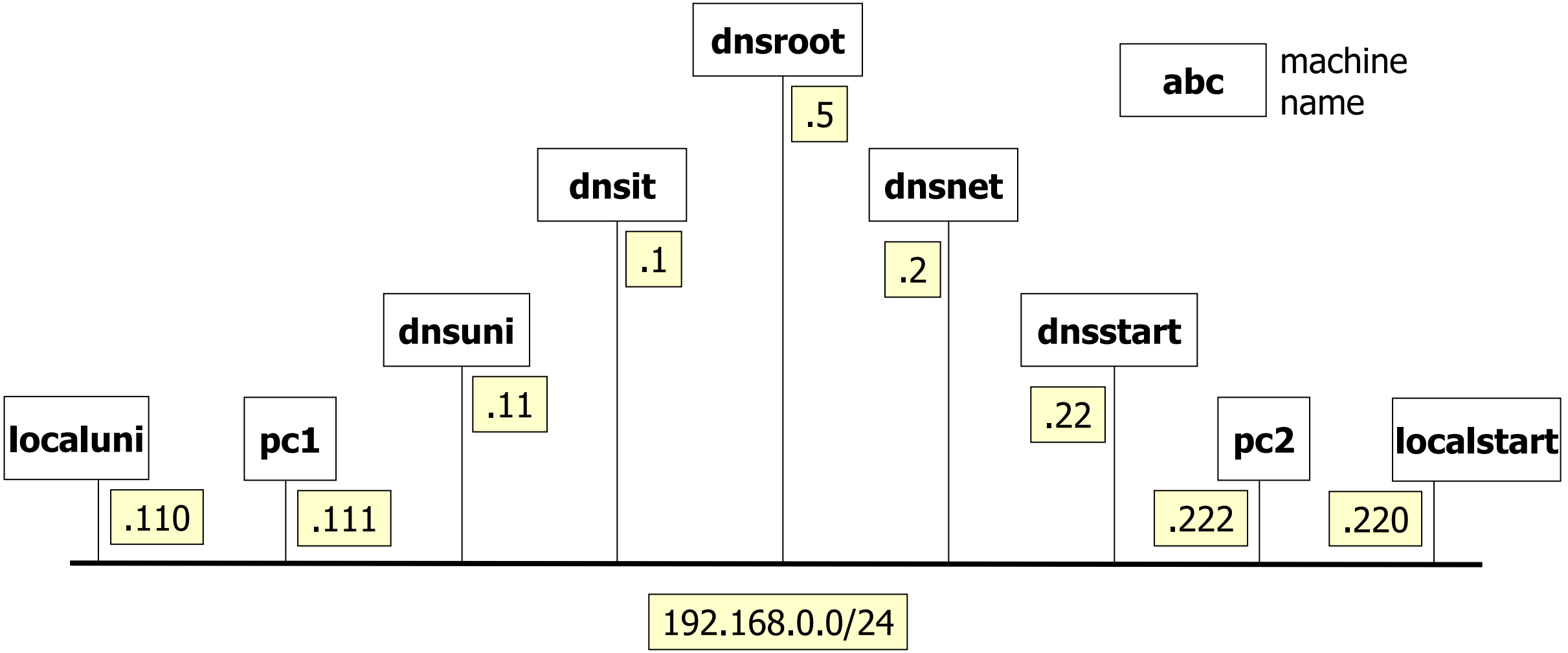


more about the DNS

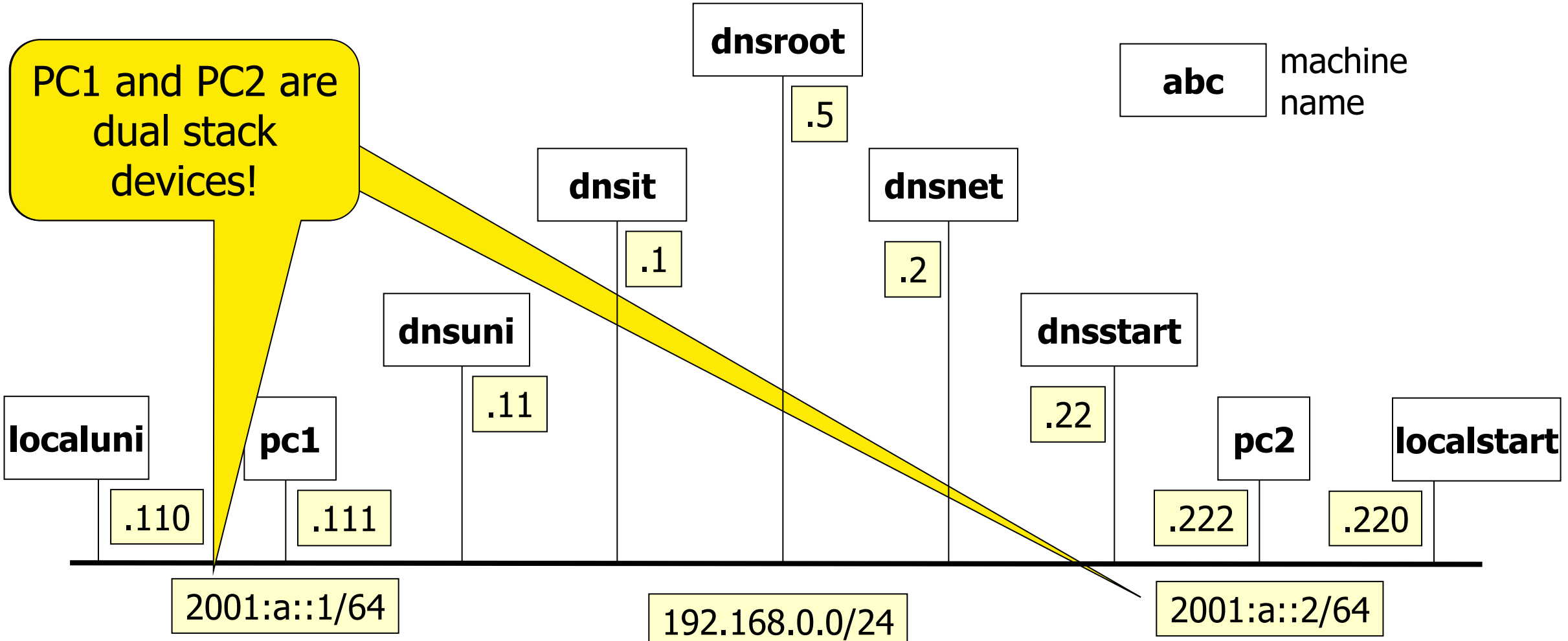
- the dns hierarchy is largely orthogonal with respect to the actual network topology
- in order to focus on the behavior of the dns we choose a flat topology, consisting of a single collision domain



step 1 – network topology (lab.conf)

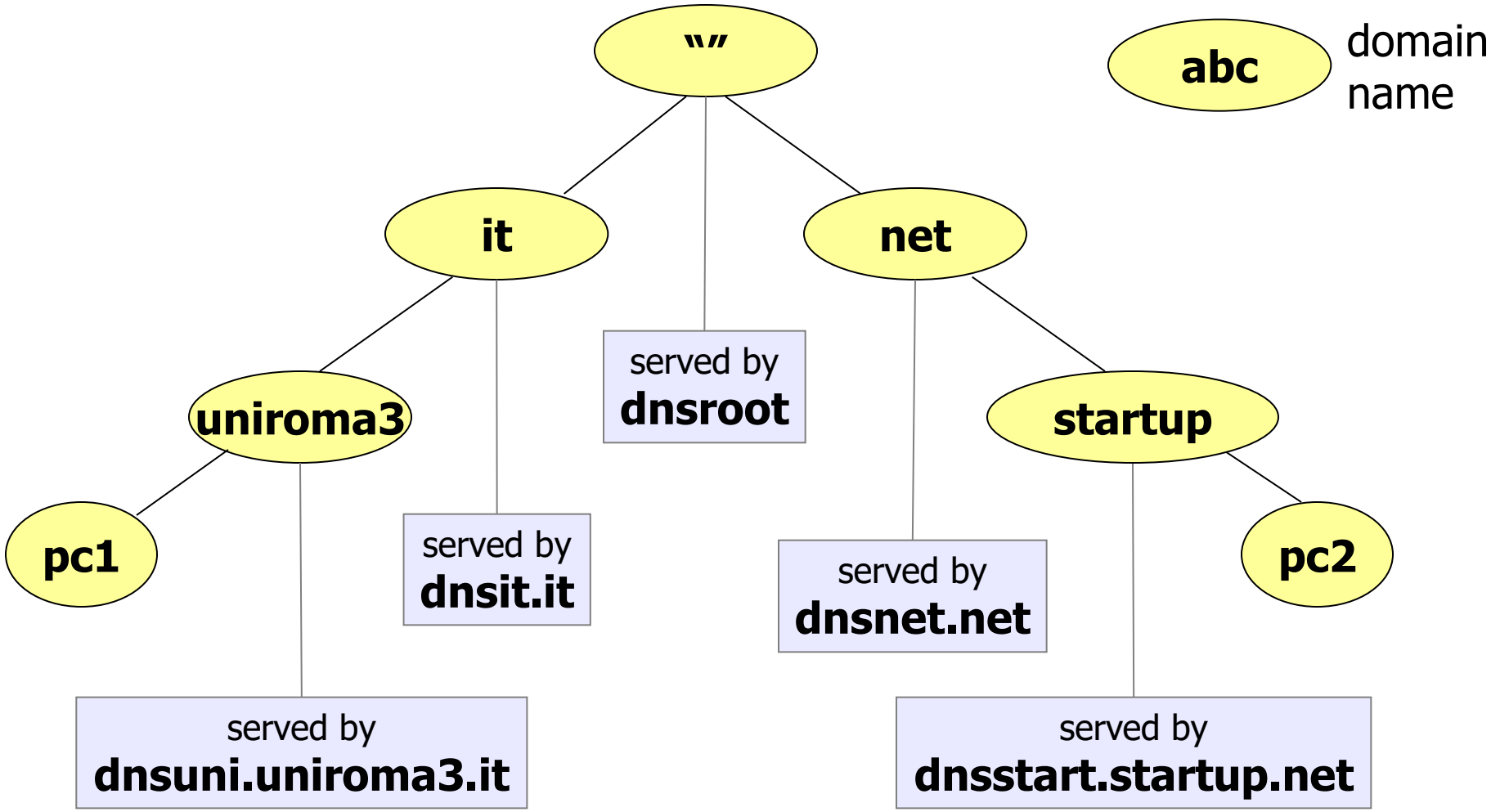


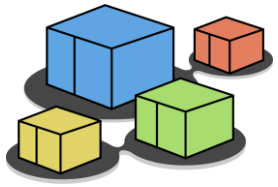
step 1 – network topology (lab.conf)



last update: Dec 2025

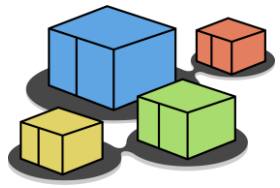
step 1 – DNS (zone) hierarchy





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

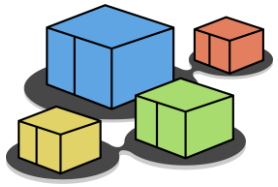
perform first IPv4 and then IPv6 queries

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

localuni.uniroma3.it

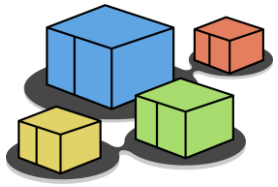
```
root@pc2:~$ cat /etc/resolv.conf
nameserver 192.168.0.220
options single-request
```

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

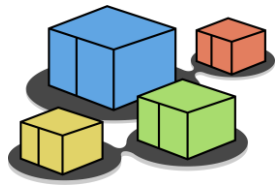
```
root@dnsuni:~$ cat /etc/bind/named.conf
include "/etc/bind/named.conf.options";

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

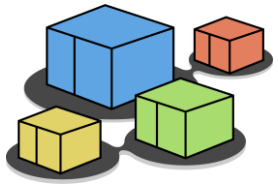


step 2 – exploring the configuration

- configuration on the name servers specifies
  - additional configuration

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

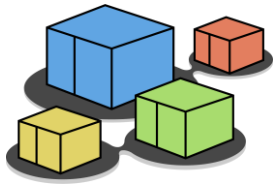
use this folder to store the cache.
COMPULSORY, otherwise, named wont 't start



format of a resource record

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

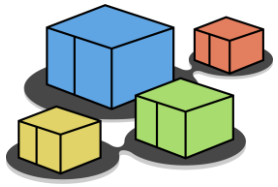
- domain: the record owner (=domain to which the record refers)
- class: usually IN (=Internet system); may be HS (=hesiod) or CH (=chaos)
- type: see next slide...
- rdata: record data (depends on the record type)



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

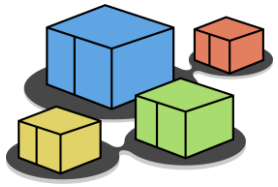


step 2 – exploring the configuration

- 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**

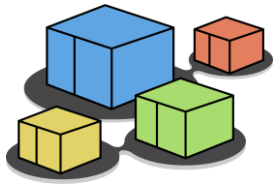


step 2 – exploring the configuration

- 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)



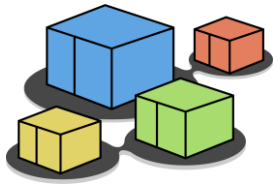
step 2 – exploring the configuration

- 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
                        )
```

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

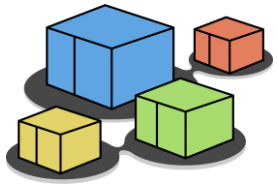
- configuration on the name servers specifies
  - authoritative information

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

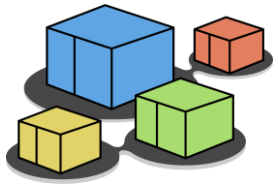


step 2 – exploring the configuration

- 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. (
                        2024120  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!



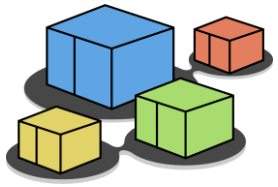
step 2 – exploring the configuration

- 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
                                   ; refresh
                                   ; retry
                                   ; 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

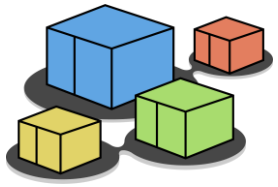


step 2 – exploring the configuration

- 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



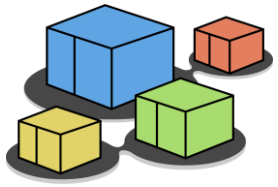
step 2 – exploring the configuration

- 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
```

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)



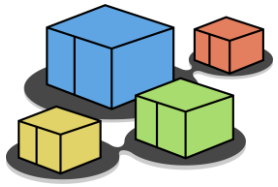
step 2 – exploring the configuration

- 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. (
                        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

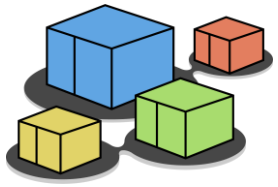


step 2 – exploring the configuration

- 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



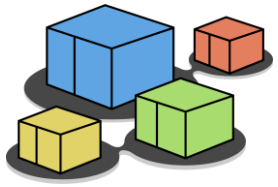
step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

ttl for negative responses from authoritative name servers

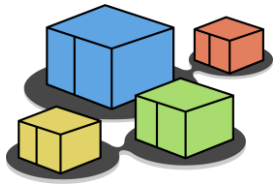
step 2 – exploring the configuration

- 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.
r                      3.it. (
                        2024120401 ;
                        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
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**

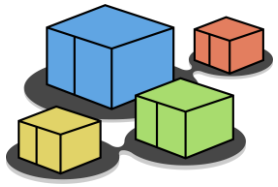


step 2 – exploring the configuration

- 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)



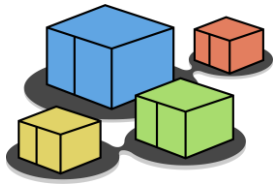
step 2 – exploring the configuration

- 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



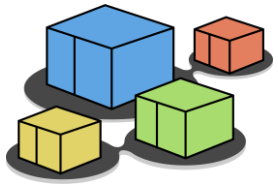
step 2 – exploring the configuration

- 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

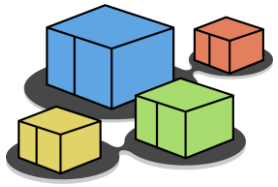
- configuration on the name servers specifies
  - allowing recursive queries and disabling dnssec

```
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;
};
```

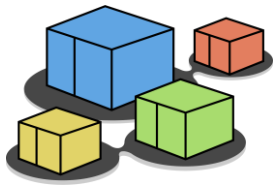
disable dnssec

allow recursive queries from `192.168.0.0/24`

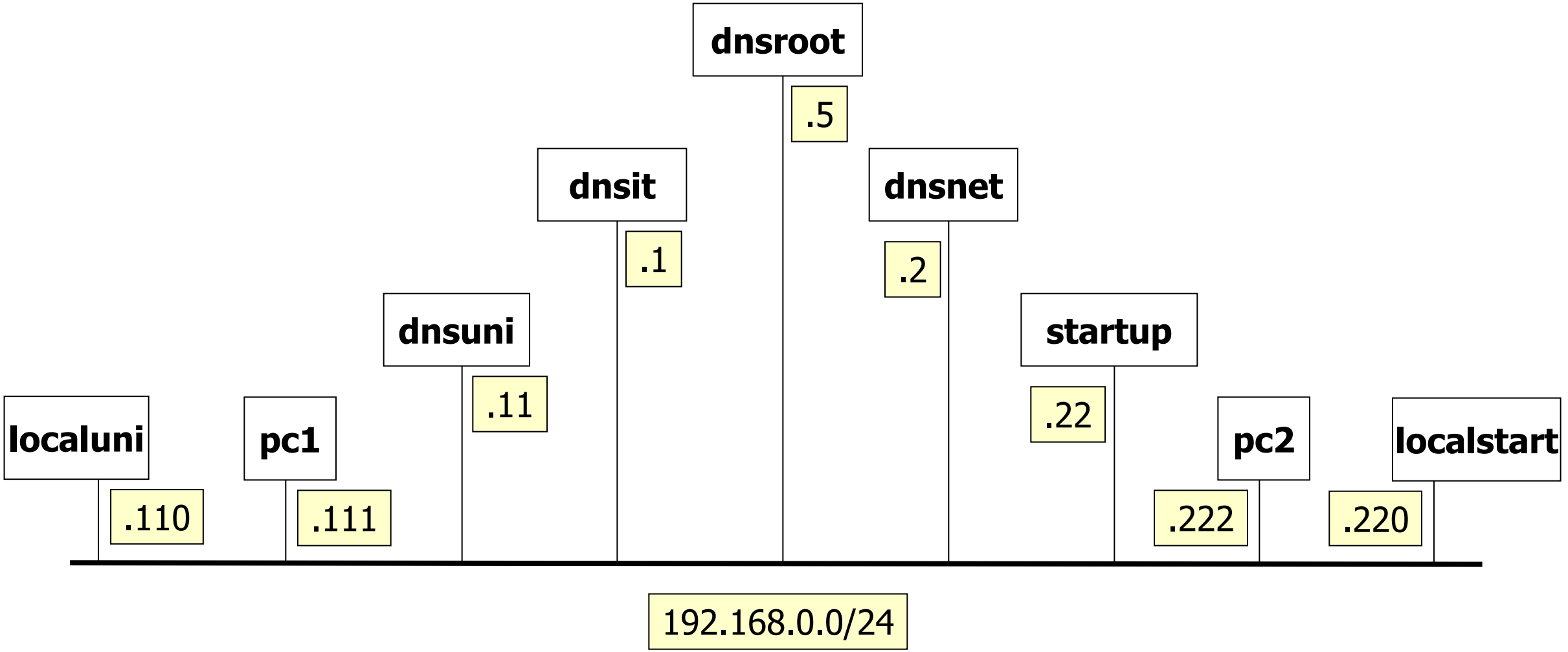
Do not send DNS cookies



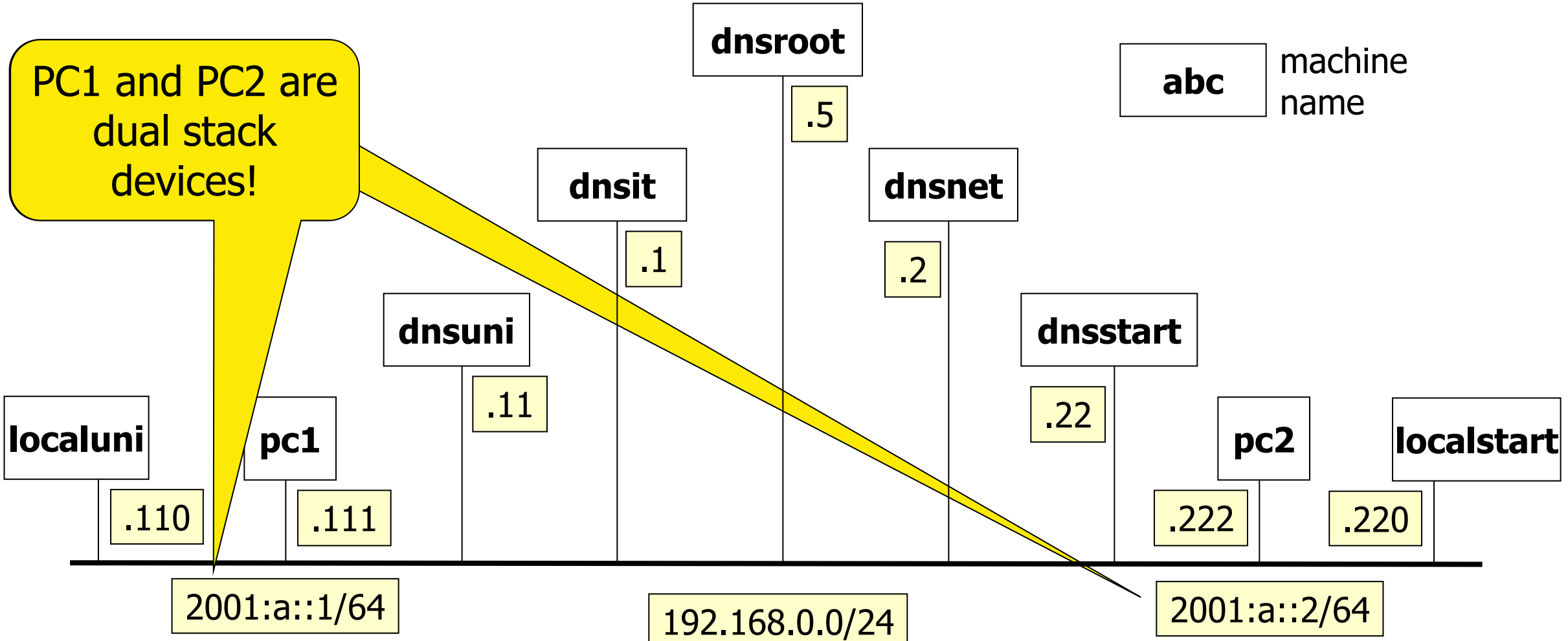
let’s start the lab



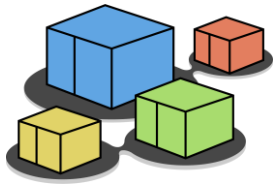
step 3 – experiment setting



step 1 – network topology (lab.conf)



last update: Dec 2025

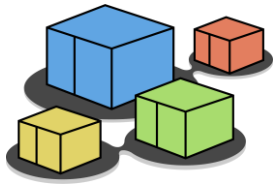


sniff the traffic

- 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



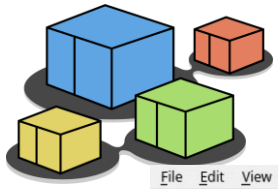
step 3 – ping from pc1

- 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 sniffer output

filter to only show DNS packets

File Edit View Go Capture Analyze Statistics Telephony Wireless Too

dns

No.	Time	Source	Destination			
3	0.000…	192.168.0.111	192.168.0.			e04 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 NS dnsstart.startup.net A 192.168.0.2…
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 192.168.0.222 OPT
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	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 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 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)
```

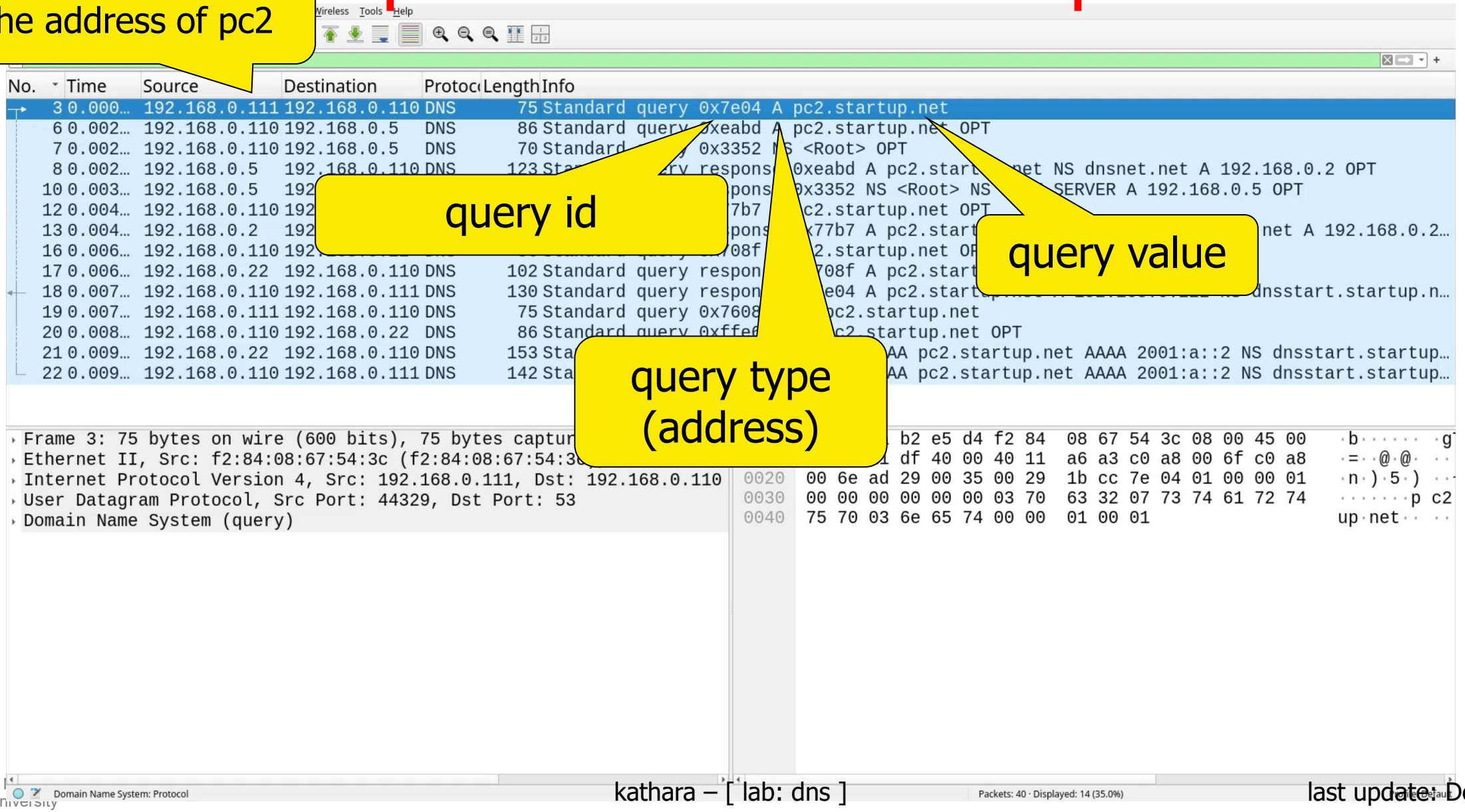
```
0000  ba 62 ca b2 e5 d4 f2 84  08 67 54 3c 08 00 45 00   ·b····· ·gT<··E·
0010  00 3d 11 df 40 00 40 11  a6 a3 c0 a8 00 6f c0 a8   ·=··@·@· ·····o··
0020  00 6e ad 29 00 35 00 29  1b cc 7e 04 01 00 00 01   ·n·)·5·) ··~·····
0030  00 00 00 00 00 00 03 70  63 32 07 73 74 61 72 74   ·······p c2·start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

Domain Name System: Protocol

Packets: 40 · Displayed: 14 (35.0%)

tep 3 – the sniffer output

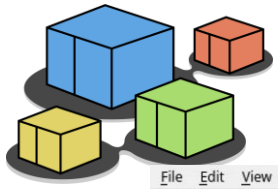
pc1 asks to **localuni** the address of pc2



query id

query value

query type (address)



step 3 – the sniffer output

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protoc	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 AAA
22	0.009…	192.168.0.110	192.168.0.111	DNS	142	Standard query response 0x7608 AAAA pc2.startup.net AAAA

request root name servers

answer with all the authoritative root name servers

```
▸ 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····· ·gT<··E·
0010  00 3d 11 df 40 00 40 11  a6 a3 c0 a8 00 6f c0 a8   ·=··@·@· ·····o··
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 74   ·······p c2·start
0040  75 70 03 6e 65 74 00 00  01 00 01                 up·net·· ···
```

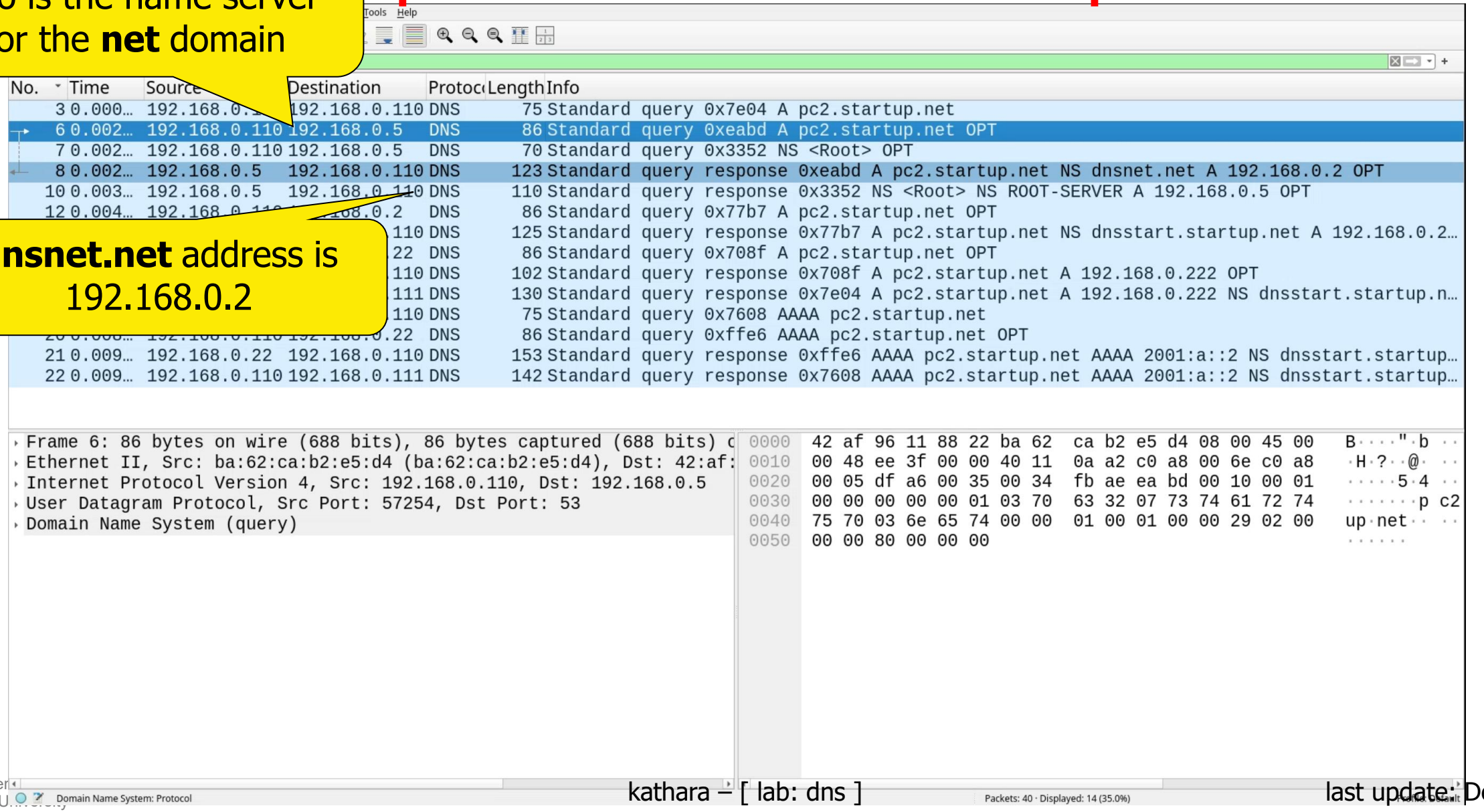
Domain Name System: Protocol

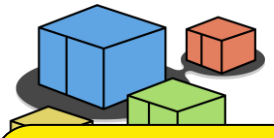
Packets: 40 · Displayed: 14 (35.0%)

ep 3 – the sniffer output

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

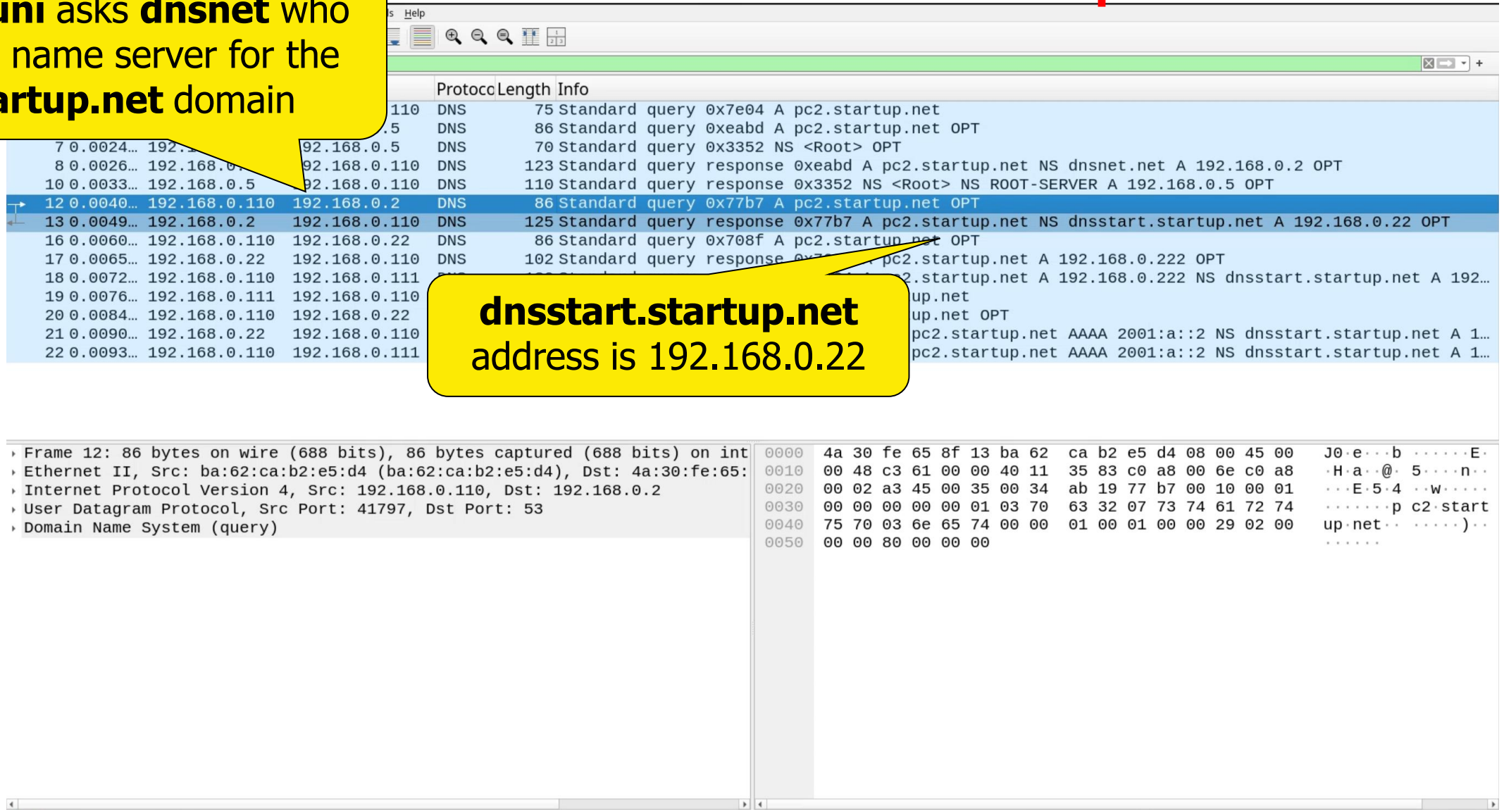
dnsnet.net address is 192.168.0.2



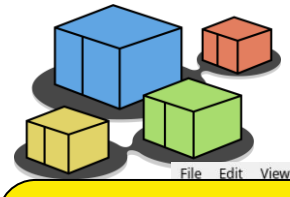


step 3 – the sniffer output

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



dnsstart.startup.net address is 192.168.0.22



step 3 – the sniffer output

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

pc2.startup.net address
is 192.168.0.222

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

				Protocc	Length	Info
			10	DNS	75	Standard query 0x7e04 A pc2.startup.net
				DNS	86	Standard query 0xeabd A pc2.startup.net OPT
				DNS	70	Standard query 0x3352 NS <Root> OPT
			110	DNS	123	Standard query response 0xeabd A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
10	0.0033…	192.168.	168.0.110	DNS	110	Standard query response 0x3352 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12	0.0040…	192.168.0.110	68.0.2	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	130	Standard query response 0x7e04 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	75	Stand…ery 0x7608 AAAA pc2.startup.net
20	0.0084…	192.168.0.1				…ffe6 AAAA pc2.startup.net OPT
21	0.0090…	192.168.0.2				…sponse 0xffe6 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup.net A 1…
22	0.0093…	192.168.0.1				…sponse 0x7608 AAAA pc2.startup.net AAAA 2001:a::2 NS dnsstart.startup.net A 1…

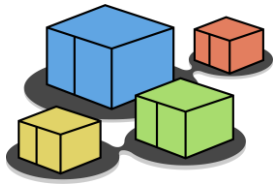
```
▸ Frame 16: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on int
▸ Ethernet II, Src: ba:62:ca:b2:e5:d4 (ba:62:ca:b2:e5:d4), Dst: 9e:e8:c9:14:
▸ Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.22
▸ User Datagram Protocol, Src Port: 58066, Dst Port: 53
▸ Domain Name System (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 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                                 ·····
```

Domain Name System: Protocol

Packets: 40 · Displayed: 14 (35.0%)

Profile: Default



step 3 – the sniffer output

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

eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

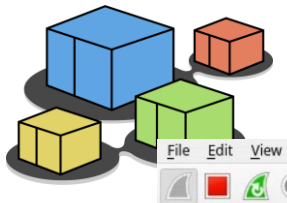
dns

No.	Time	Source	Destination	Protocol	Length	Info
				DNS	75	Standard query 0xb5d4 A pc2.startup.net
				DNS	86	Standard query 0x8ff1 A pc2.startup.net OPT
				DNS	70	Standard query 0x7d19 NS <Root> OPT
				DNS	123	Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
				DNS	110	Standard query response 0x7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
				DNS	86	Standard query 0x5ac0 A pc2.startup.net OPT
13	0.008519351	192.1	.168.0.110	DNS	125	Standard query response 0x5ac0 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
16	0.009507968	192.168.0	92.168.0.22	DNS	86	Standard query 0x4bba A pc2.startup.net OPT
17	0.009914852	192.168.0.22	192.168.0.110	DNS	102	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 OPT
18	0.010656291	192.168.0.110	192.168.0.111	DNS	130	Standard query response 0xb5d4 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
19	0.010932933	192.168.0.111	192.168.0.110	DNS	75	Standard query 0xeccb AAAA pc2.startup.net
20	0.011471405	192.168.0.110	192.168.0.22	DNS	86	Standard query 0x722b AAAA pc2.startup.net OPT
21	0.011875739	192.168.0.22	192.168.0.110	DNS	136	Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
22	0.012129873	192.168.0.110	192.168.0.111	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 74   ·······p  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                                             ··
```

Text item (text), 16 byte(s) — Packets: 40 · Displayed: 14 (35.0%) — Profile: Default



step 3 – the sniffer output

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
3	0.0007…	192.168.0.111	192.168.0.110	DNS	75	Standard query 0x7e04 A pc2.startup.net
					86	Standard query 0xeabd A pc2.startup.net OPT
					70	Standard query 0x3352 NS <Root> OPT
					123	Standard query response 0xeabd A pc2.startu
					110	Standard query response 0x3352 NS <Root> NS
					86	Standard query 0x77b7 A pc2.startup.net OPT
					125	Standard query response 0x77b7 A pc2.sta
16	0.0060…	192.168.0.110		DNS	86	Standard query 0x708f A pc2.startup
17	0.0065…	192.168.0.22	192	DNS	102	Standard query response 0x708f A
18	0.0072…	192.168.0.110	192.168.0.111	DNS	130	Standard query response 0x7e04 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	75	Standard query 0x7608 AAAA pc2.startup.net
20	0.0084…	192.168.0.110	192.168.0.22	DNS	86	Standard query 0xffe6 AAAA pc2.startup.net OPT
21	0.0090…	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.net A 1…
22	0.0093…	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.net A 1…

Frame 19: 75 wire (600 bits), 75 bytes captured (600 bits) on int
Ethernet II, :08:67:54:3c (f2:84:08:67:54:3c), Dst: ba:62:ca:b2:
Internet Pro 4, Src: 192.168.0.111, Dst: 192.168.0.110
User Datagra Port: 44329, Dst Port: 53
D

Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 22]

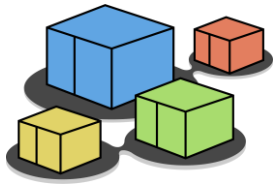
0000 ba 6 E·
0010 00 3 ··
0020 00 6 ··
0030 00 0 rt
0040 75 7

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**



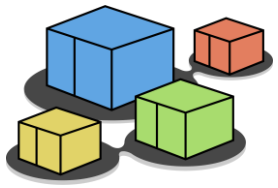
step 3 – ping from pc1

- execute a ping6 command towards pc2

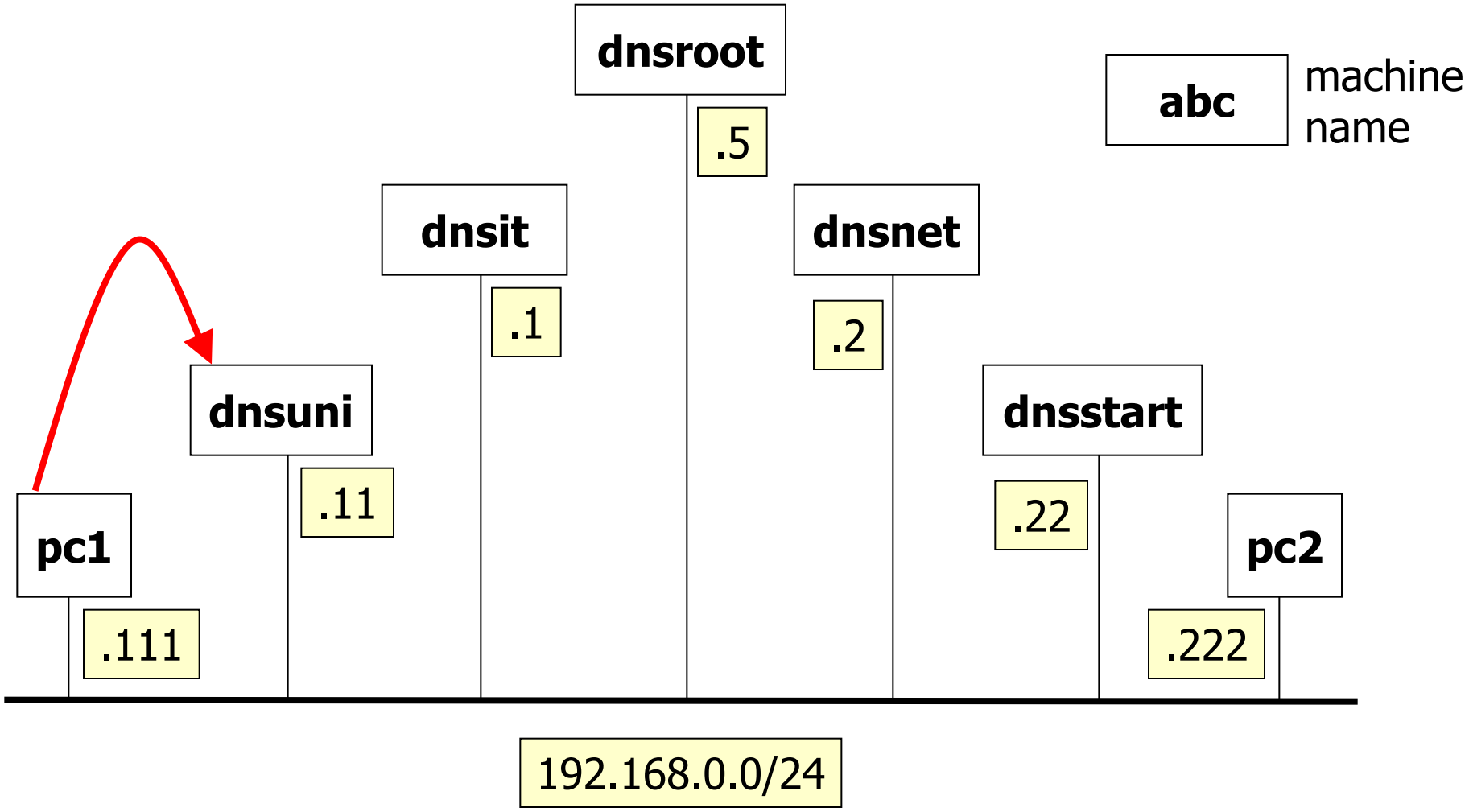
Ping using IPv6 addresses

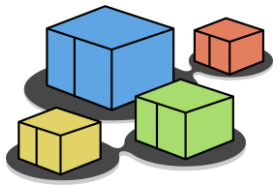
pc1

```
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
```

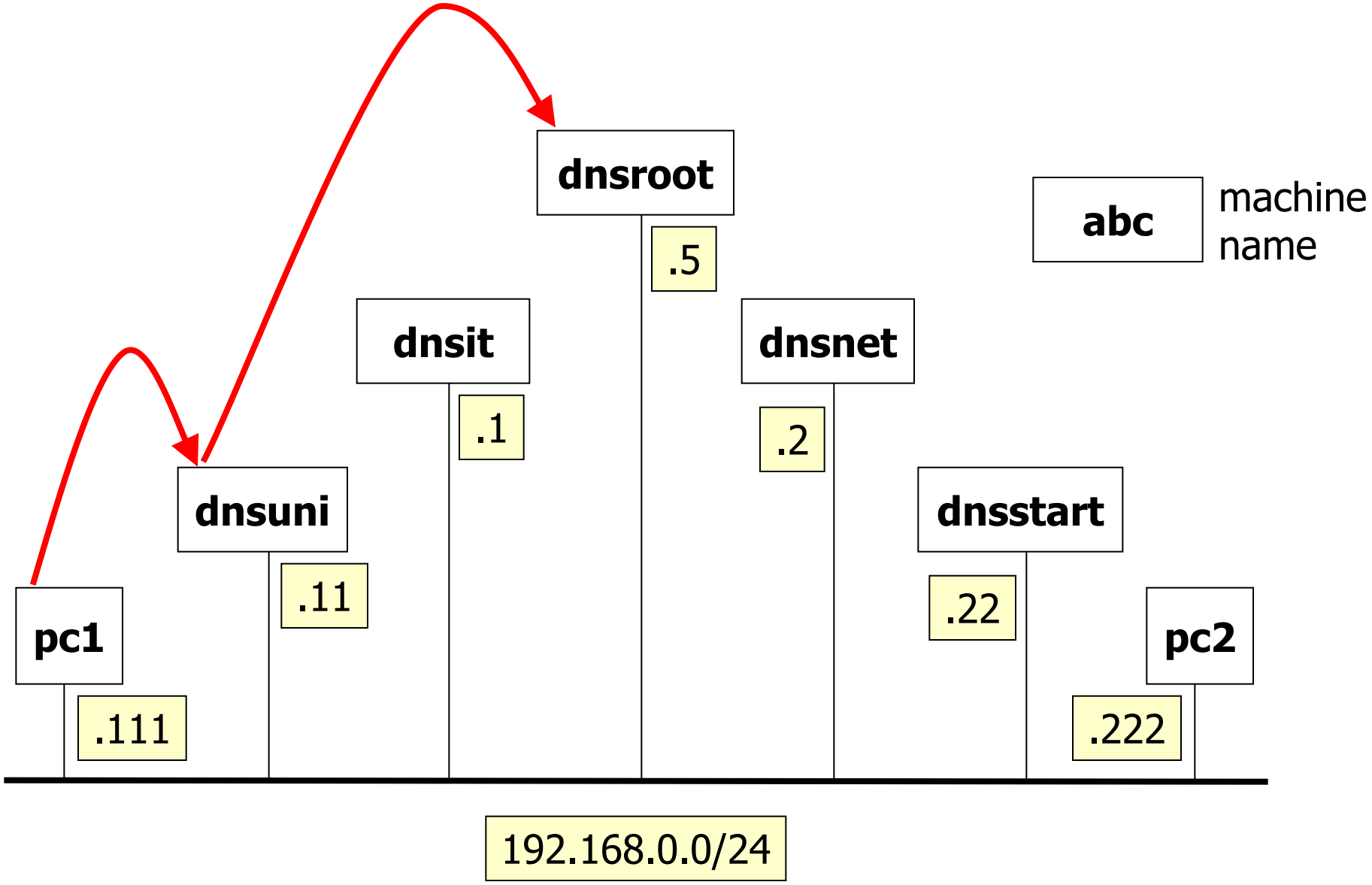


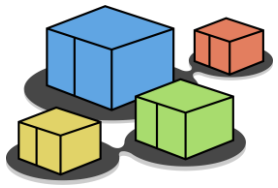
step 3 – exchanged messages



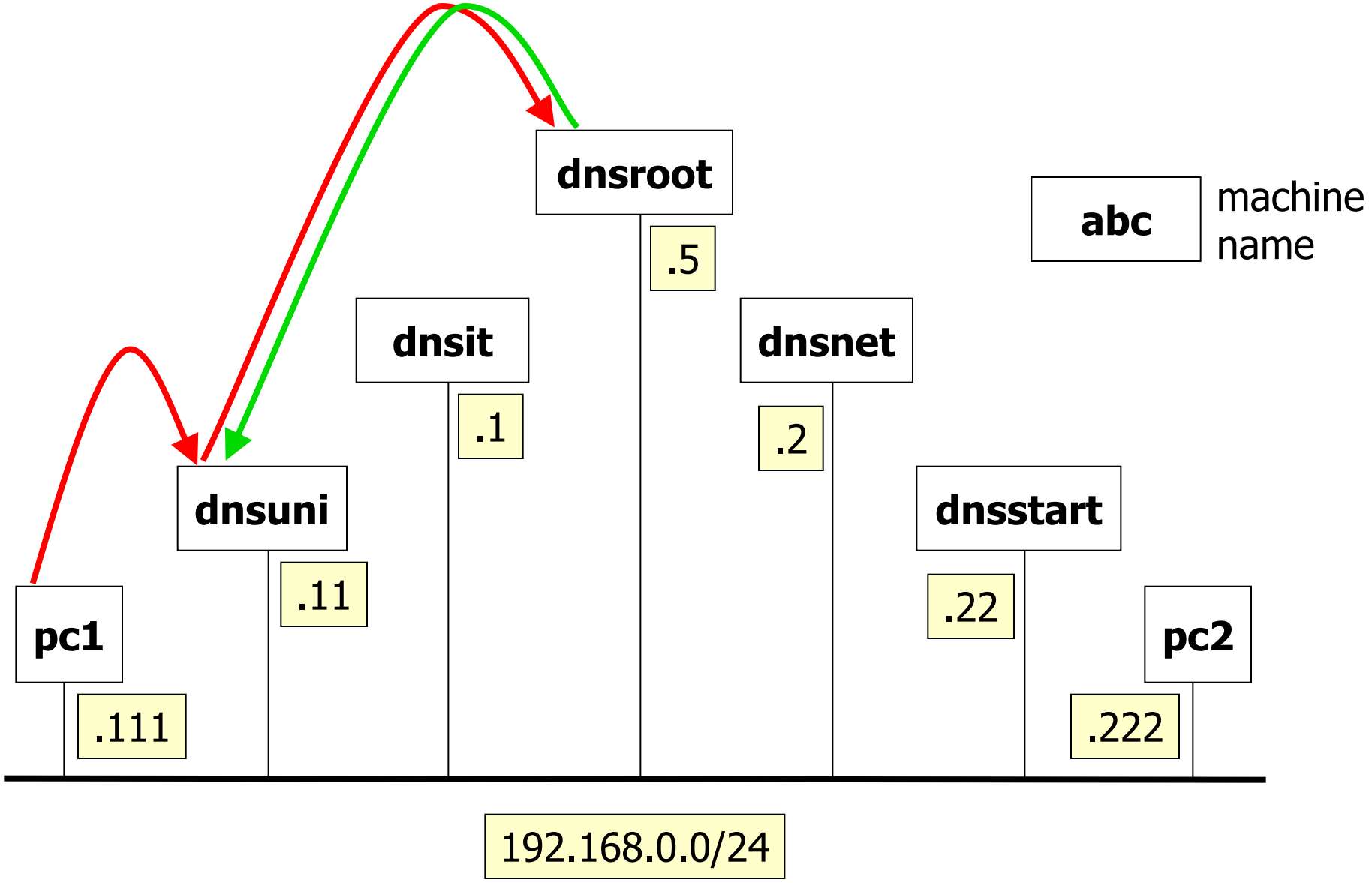


step 3 – exchanged messages

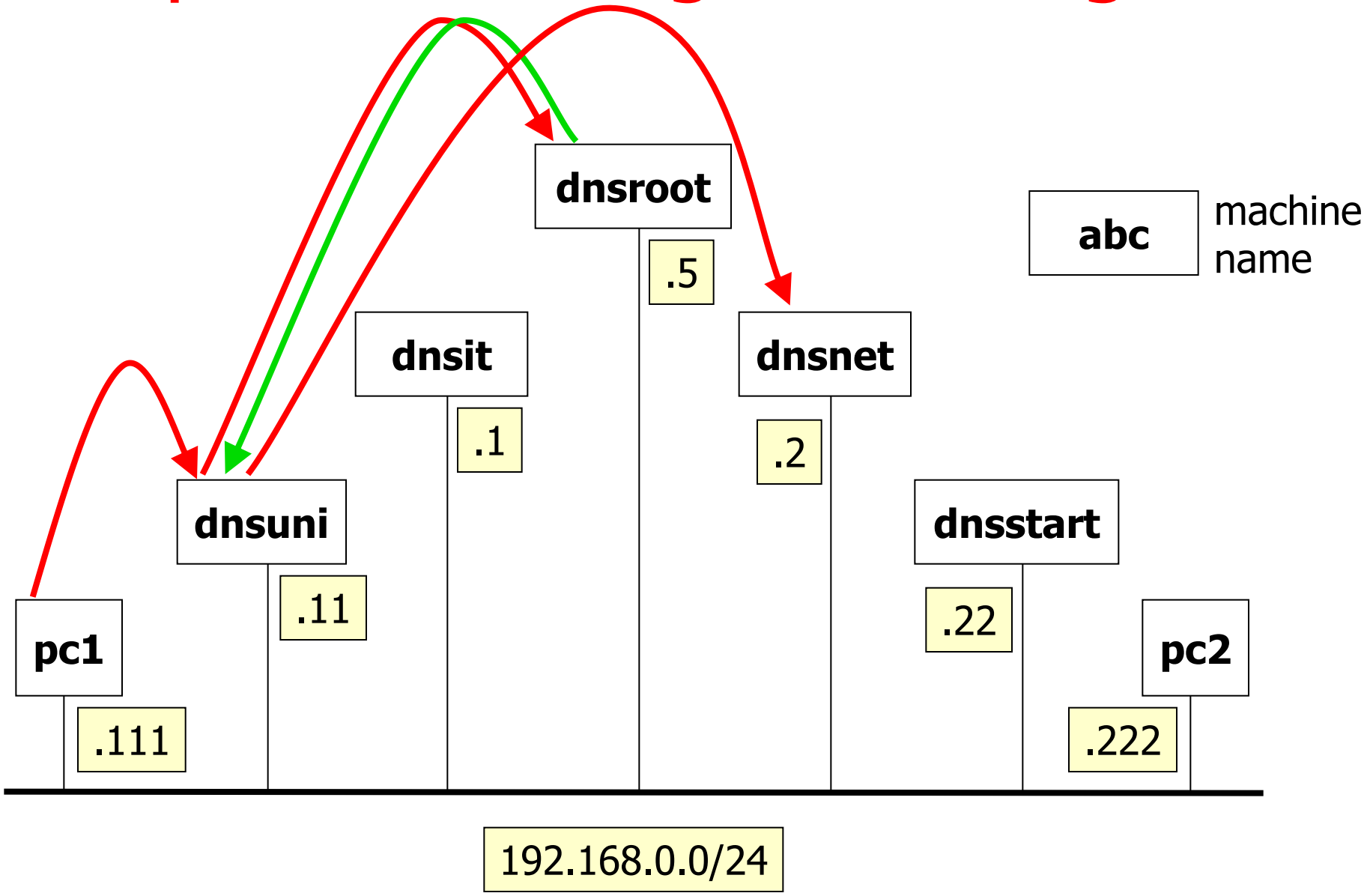


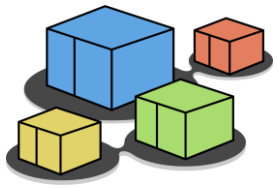


step 3 – exchanged messages

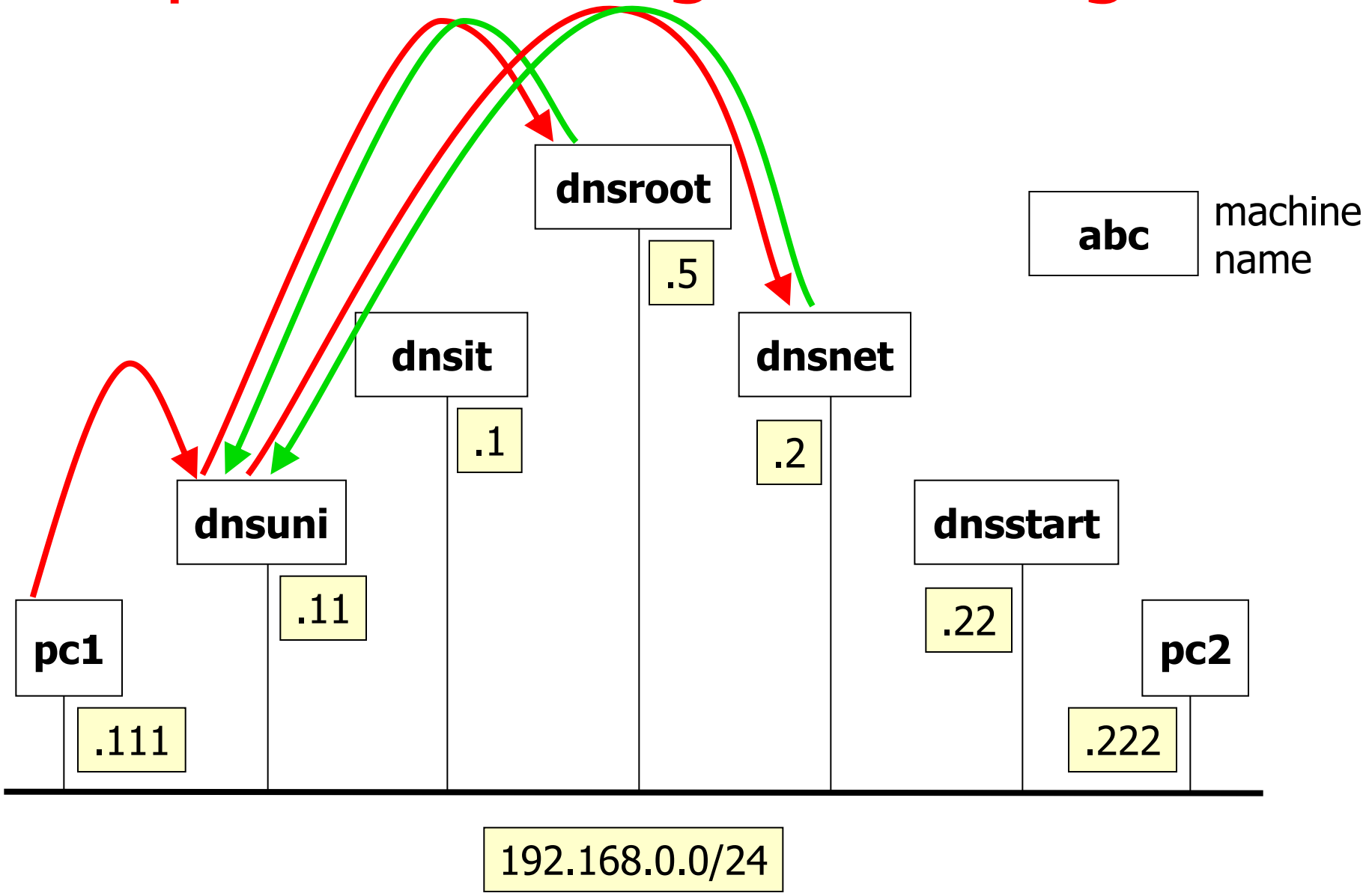


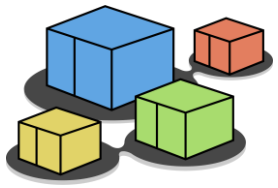
step 3 – exchanged messages



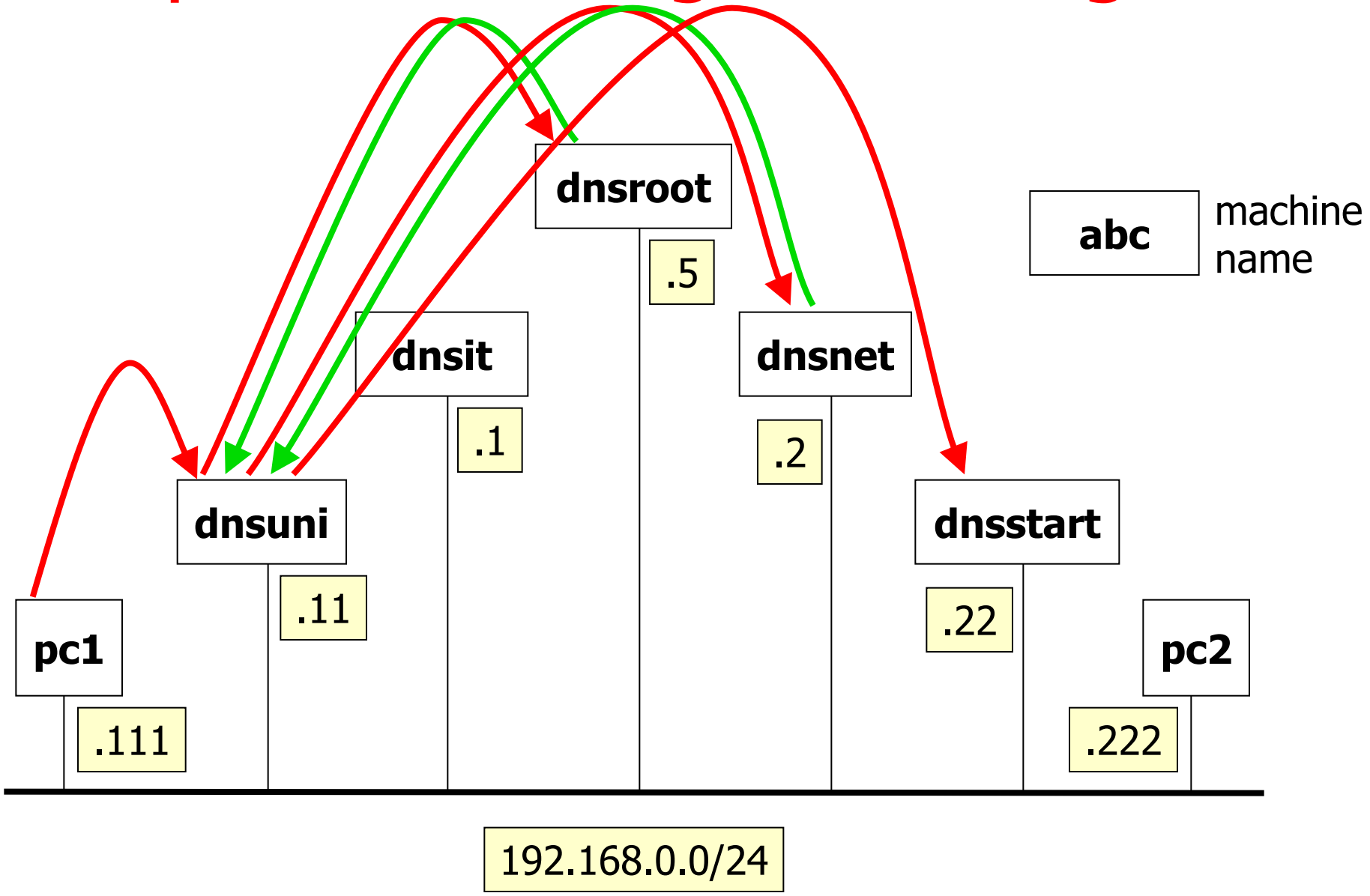


step 3 – exchanged messages

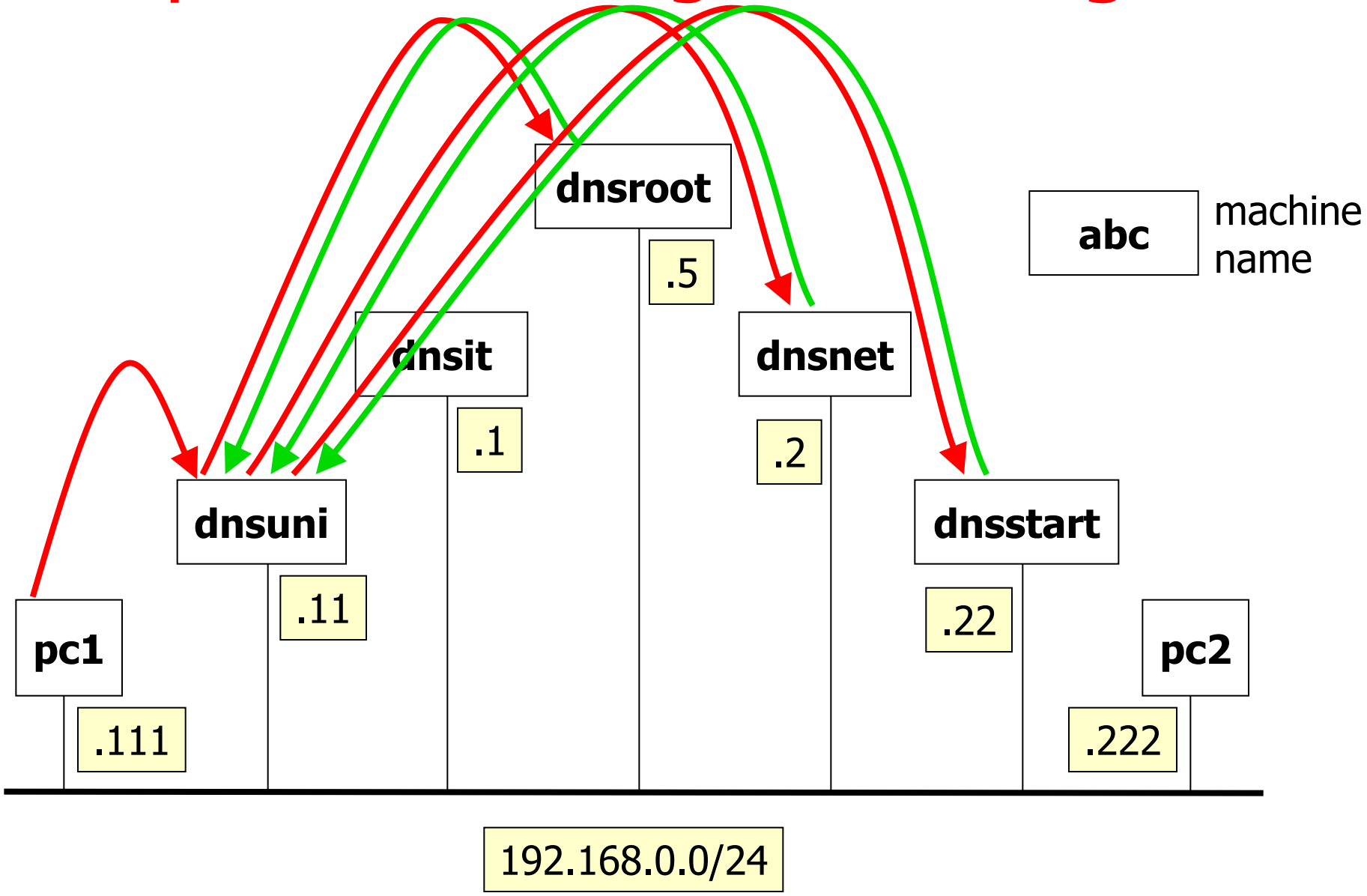




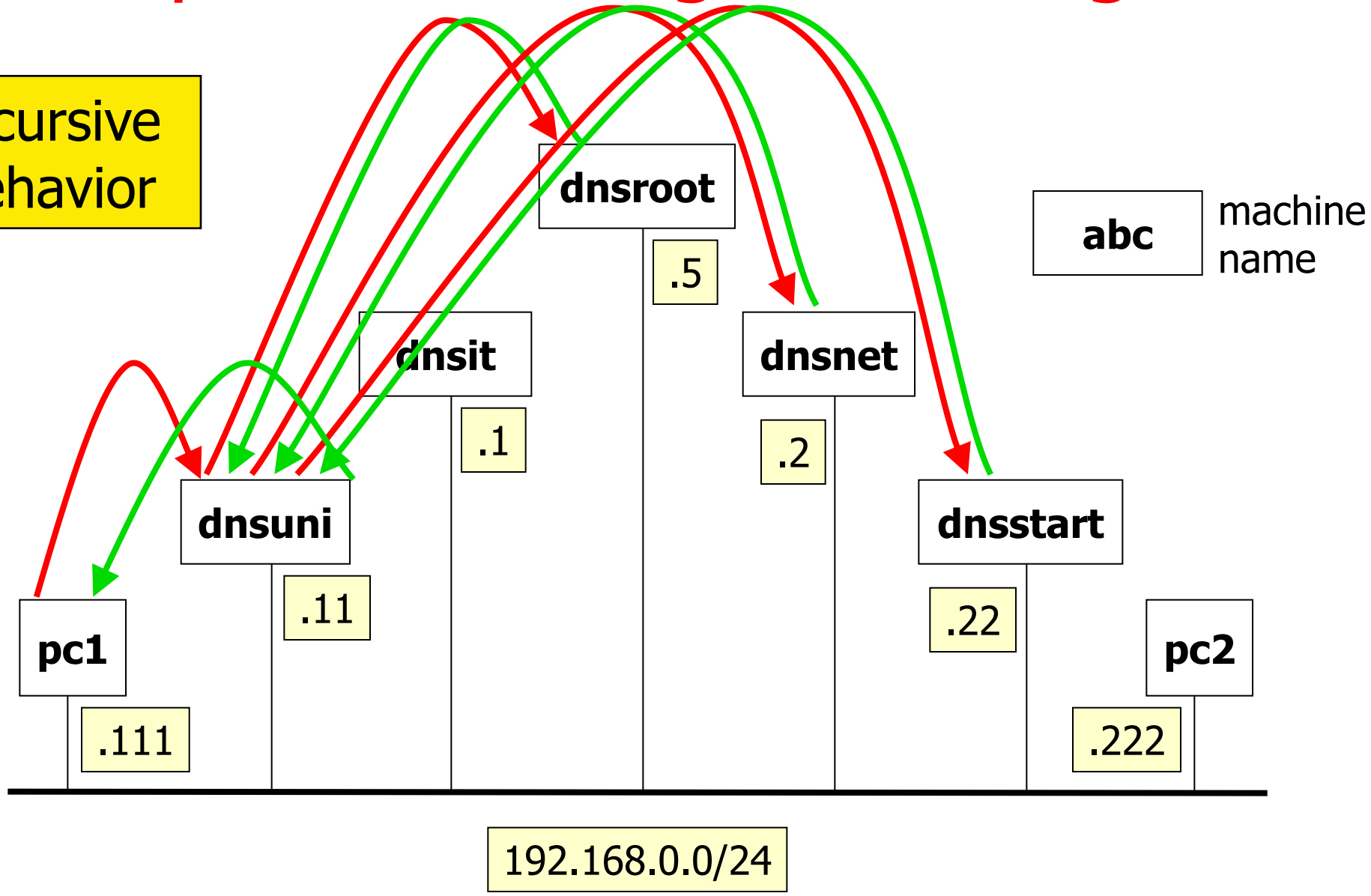
step 3 – exchanged messages

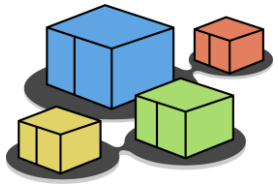


step 3 – exchanged messages



step 3 – exchanged messages



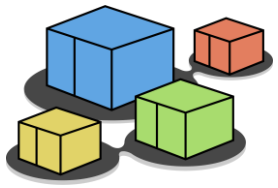


step 4 – repeating the experiment

- 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	168.0.111	DNS	125	Standard query response 0x9e05 AAAA pc2.startup.net SOA dnsstart.startup.net

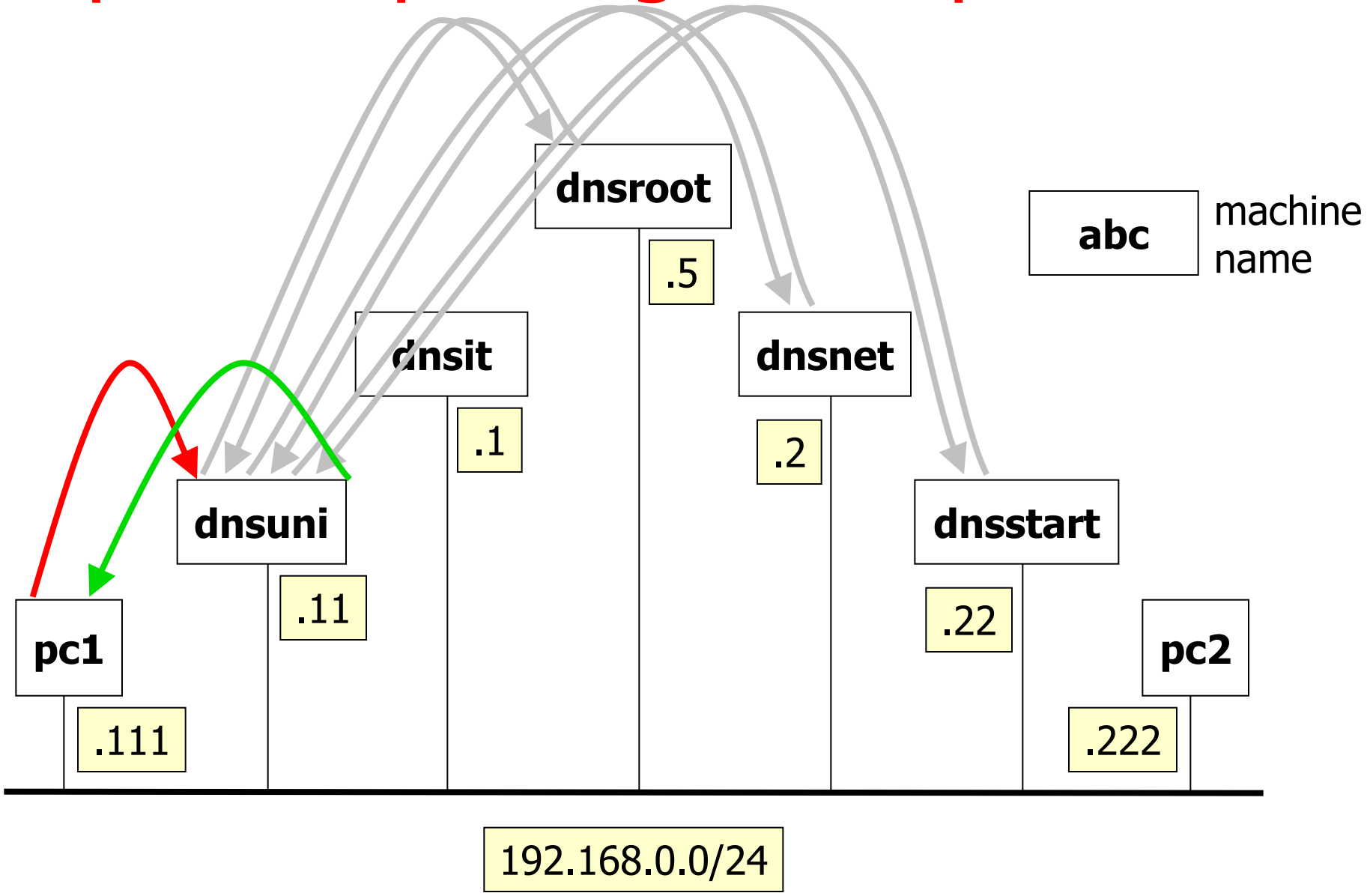
the name server cache helps reducing traffic

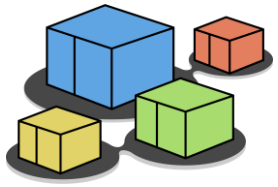
```
Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et
Ethernet II, Src: 92:93:6c:69:91:fc (92:93:6c:69:91:fc), Dst: ee:d6:b8:29:cf:ae (e
Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110
User Datagram Protocol, Src Port: 35784, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x591b
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 2]
```

```
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 74   ·······p 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



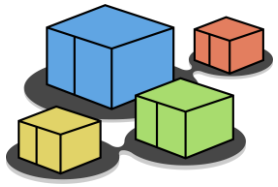


step 5 – cleaning the cache

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

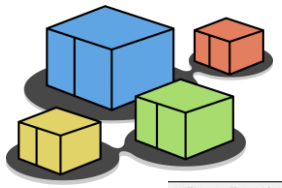


step 6 – ping non-existent target

- 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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

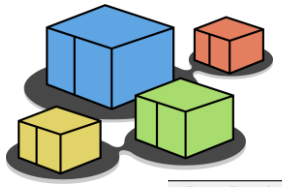
dns

No.	Time	Source	Destination	Proto	Lengt	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	192.168.0.2	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 O…
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		Standard query 0xb4a0 AAAA pluto.startup.net
12	0.0…	192.168.0.110	192.168.0.111	DNS		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: f2:84:08:67:54:3c
▸ Internet Protocol Version 4, Src: 1
▸ User Datagram Protocol, Src Port: 4
▾ 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 T<···E·
45 40 00 40 11  dc 3a c0 a8 00 6f c0 a8   E@·@··:· ···o··
e3 00 35 00 2b  c2 bb 5c a4 01 00 00 01   ··5·+··\ ····
00 00 00 05 70  6c 75 74 6f 07 73 74 61   ····plut o·sta
70 03 6e 65 74  00 00 01 00 01            p·net··· ··
```



step 6 – non-existent target

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

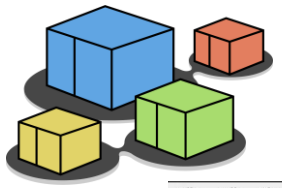
dns

No.	Time	Source	Destination	Proto	Lengt	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 O…
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 0xb4 0 AAAA pluto.startup.net
12	0.0…	192.168.0.110	192.168.0.111	DNS	127	Standard query respo 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: 192.168.0.1
▸ 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]
```

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

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



step 6 – non-existent target

pc1 asks **localuni** for AAAA records of **pluto.startup.net**

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

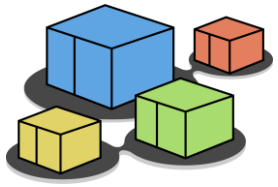
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Proto	Lengt	Info
1	0.0…	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x5ca4 A pluto.startup.net
2	0.0…	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x2cb4 A pluto.startup.net OPT
3	0.0…	192.168.0.111	192.168.0.110	DNS	77	Standard query 0xd75d NS <Root> OPT
4	0.0…	192.168.0.110	192.168.0.111	DNS	127	Standard query response 0x2cb4 A pluto.startup.n…
5	0.0…	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x6ee4 A pluto.startup.net OPT
6	0.0…	192.168.0.5	192.…	DNS	110	Standard query response 0xd75d NS <Root> N…
7	0.0…	192.168.0.2	192.168…	DNS	127	Standard query response 0x6ee4 A pluto… tup.n…
8	0.0…	192.168.0.110	192.168.0.2	DNS	88	Standard query 0xbe7c A pluto.start… .net OPT
9	0.0…	192.168.0.22	192.168.0.110	DNS	138	Standard query response 0xbe7c N… such name A pluto.startup.net SOA dnsstart.startup.net O…
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) 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: 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]
```

```
0000  ba 62 ca b2 e5 d4 f2 84  08 67 54 3c 08 00 45 00   ·b······ ·gT<··E·
0010  00 3f dc 45 40 00 40 11  dc 3a c0 a8 00 6f c0 a8   ·?·E@·@· ·:···o··
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 luto·sta
0040  72 74 75 70 03 6e 65 74  00 00 01 00 01           rtup·net ·····
```

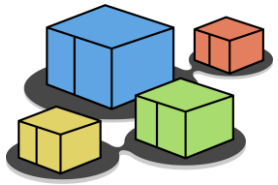


step 6 – ping non-existent target

- 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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

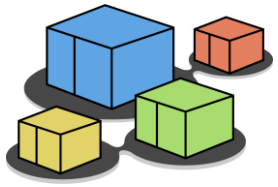
dns
dnsserver

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000…	192.168.0…	192.168.0…	DNS	77	Standard query … A pluto.startup.net
2	0.000…	192.168.0…	192.168.0…	DNS	127	Standard query response 0xeb70 No such name A pluto.startup.net SOA dnsstart.startup.net
3	0.001…	192.168.0…	192.168.0…	DNS	77	Standard query 0xeb07 AAAA pluto.startup.net
4	0.001…	192.168.0…	192.168.0…	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 bit
▸ 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]
```

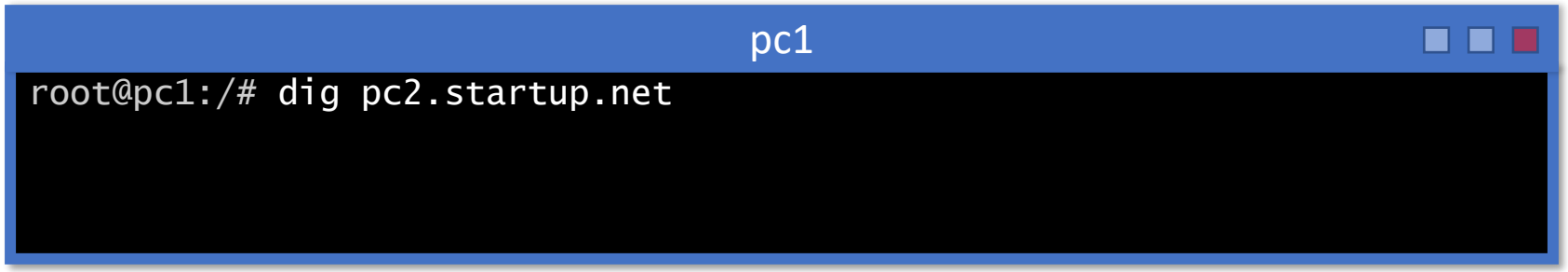
```
0000  8e e3 c4 b3 07 17 da e3  47 a3 3c 22 08 00 45 00   ........ G·<"··E·
0010  00 71 3a ea 00 00 40 11  bd 64 c0 a8 00 6e c0 a8   ·q:···@· ·d···n··
0020  00 6f 00 35 83 27 00 5d  44 25 eb 70 81 83 00 01   ·o·5·'·] D%·p····
0030  00 00 00 01 00 00 05 70  6c 75 74 6f 07 73 74 61   ·······p luto·sta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

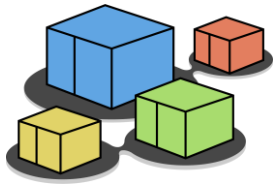
Domain Name System: Protocol — Packets: 8 · Displayed: 4 (50.0%) — Profile: Default



step 7 – advanced queries

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



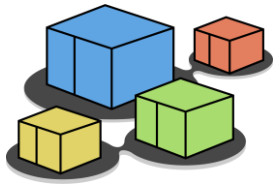


step 7 – advanced queries

Request ANY type of record

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
```

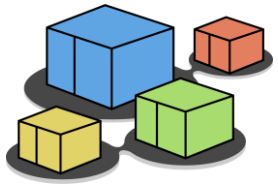


step 7 – advanced queries

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
```

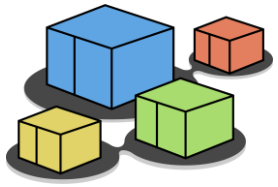


step 7 – advanced queries

these sections correspond to those contained in DNS packets

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
```



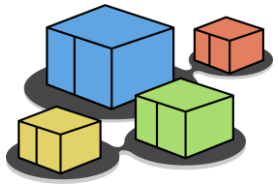
step 7 – advanced queries

records 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

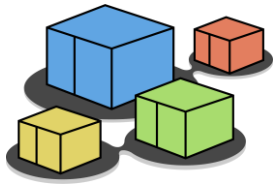
may be more than one

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

                                NS      dnsstart.startup.net.

                                IN      A       192.168.0.22
```

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`**)



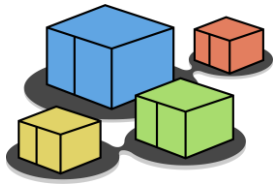
step 7 – advanced queries

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
```

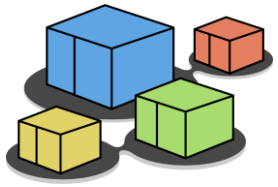
- perform an iterative query using **dig**

pc1

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

avoid displaying question and additional sections

disable recursion

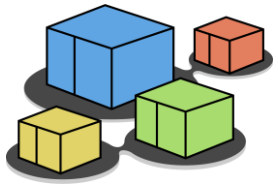


step 8 – an iterative query

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
```



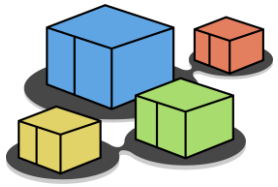
step 8 – an iterative query

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

; <<>> DiG 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
```



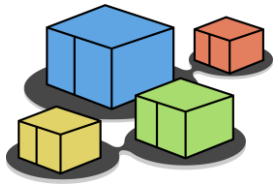
step 8 – an iterative query

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 9.18.19-1~deb12u1-Debian <<>> +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~deb12 <<>> +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
```