



# kathara lab

## DNS

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

© Computer Networks Research Group  
Roma Tre University

1



# 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.

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

2



## 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
- all IP addresses are IPv4



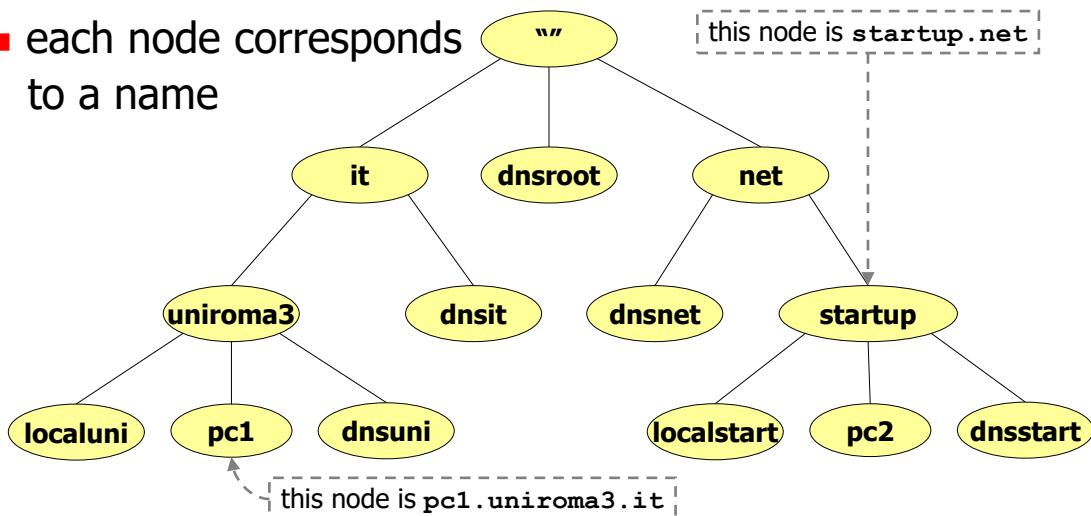
## about the DNS

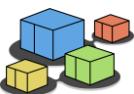
- takes care of associating names with IP addresses
- the **name system** is distributed over several nodes (hosts) that are hierarchically organized to form a tree
- each node in the hierarchy corresponds to a **name**
- a **domain** in the name system is a subtree
- a node in the hierarchy may be delegated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

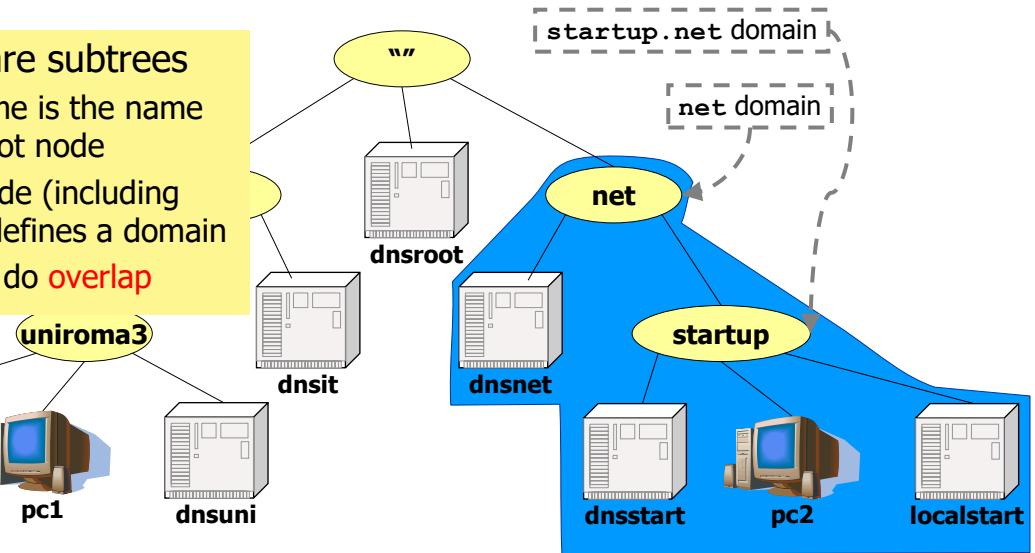
- each node corresponds to a name





# 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**



© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

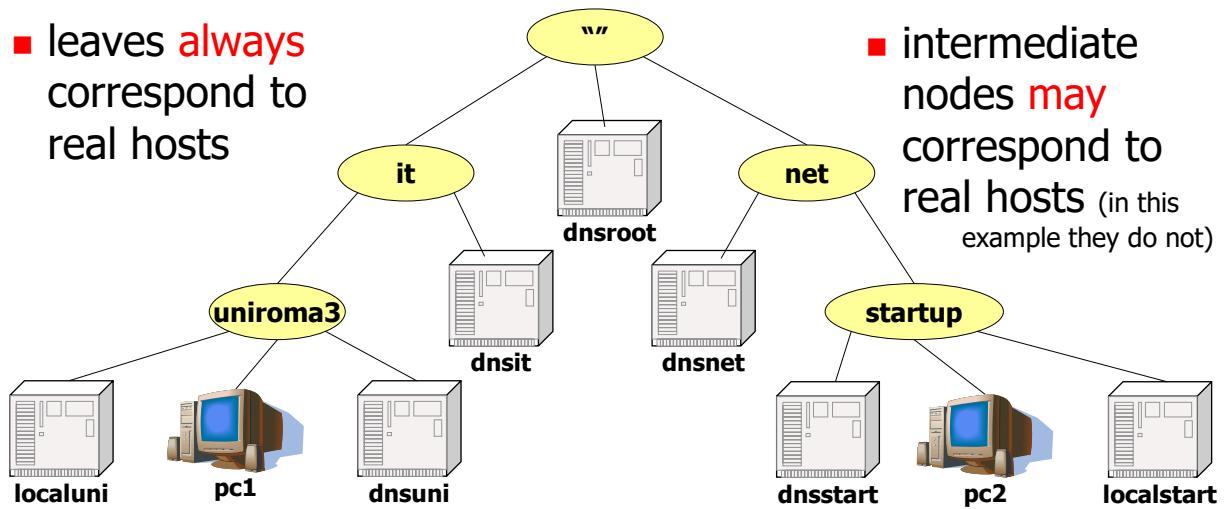
7



# the DNS name hierarchy

- leaves **always** correspond to real hosts

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



© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

8

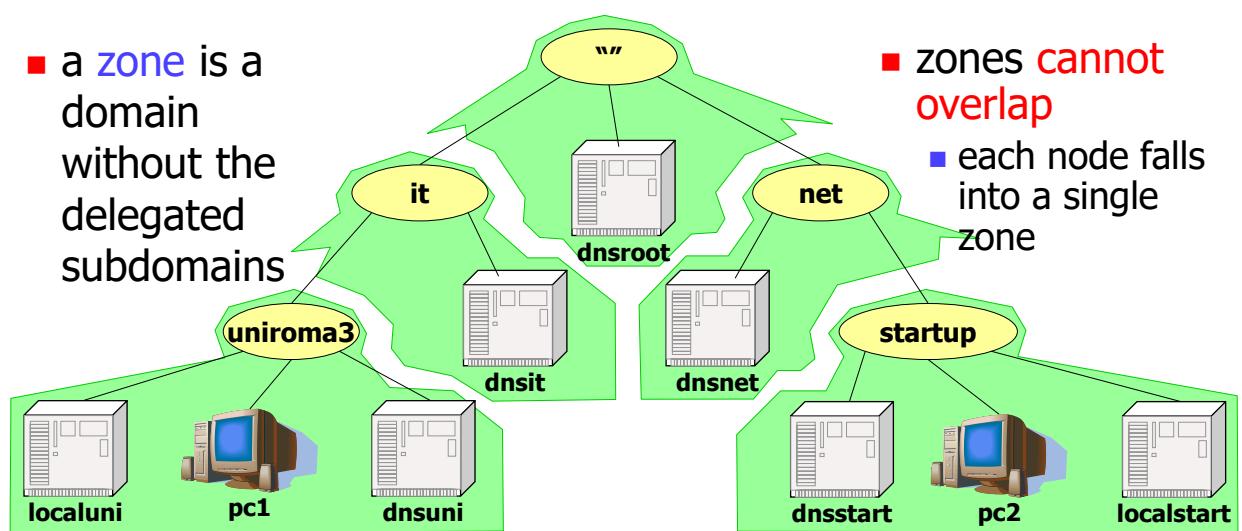


## zones

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

- **zones cannot overlap**

- each node falls into a single zone



© Computer Networks Research Group  
Roma Tre University

kathara - [ lab: dns ]

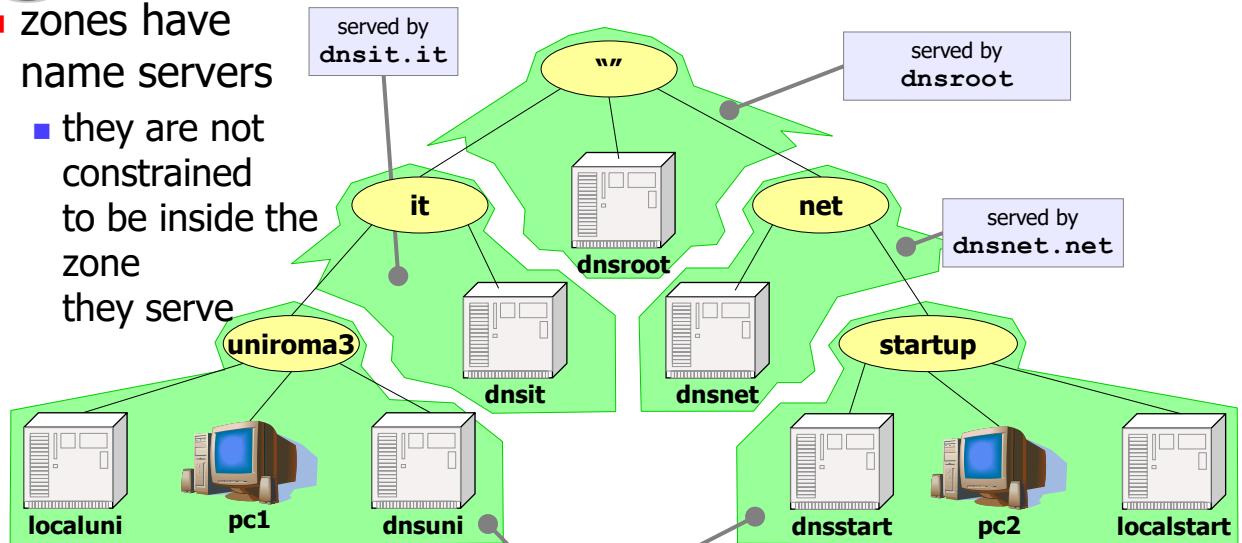
last update: Dec 2023

9



## zones

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



© Computer Networks Research Group  
Roma Tre University

kathara - [ lab: dns ]

last update: Dec 2023

10

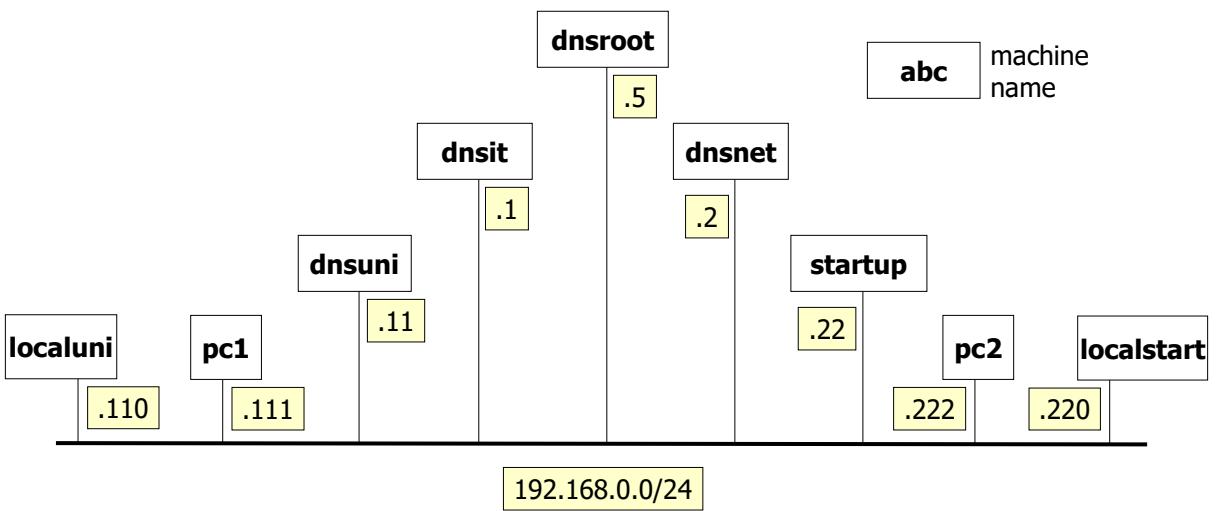


## more about the DNS

- 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

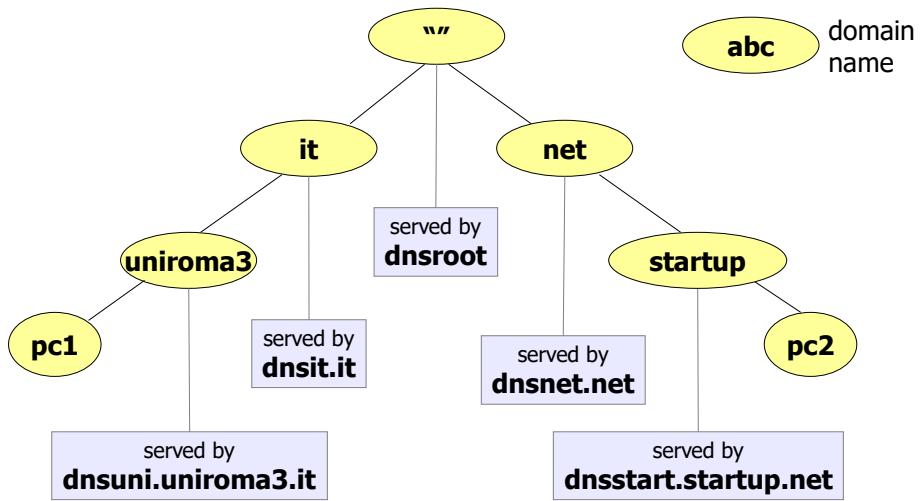


## step 1 – network topology





## step 1 – DNS (zone) hierarchy



© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

13



## 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*

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

14



## 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
search uniroma3.it
options single-request
```

localuni.uniroma3.it

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

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

<b>A</b>	a host address.
A6	Obsolete format of IPv6 address.
<b>AAAA</b>	an IPv6 address.
AFSDB	(x) location of AFS database servers. Experimental.
CERT	holds a digital certificate.
<b>CNAME</b>	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.
<b>MX</b>	identifies a mail exchange for the domain. See RFC 974 for details.
NAPTR	name authority pointer.
NSAP	a network service access point.
<b>NS</b>	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.
<b>SOA</b>	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. (
            2006031201 ; 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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

23



## 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";
};
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

24



## step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

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. (
                          2006031201 ; serial
                          28 ;
```

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. (
    2006031201 ; 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. (
    2006031201 ; serial
    28 ; refresh
```

serial number

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



## step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

refresh interval  
(seconds)

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



## step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

interval (seconds)  
between  
subsequent  
attempts to  
contact the master



## step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

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

slave expire time (seconds)



## step 2 – exploring the configuration

- configuration on the name servers specifies
  - authoritative information

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

ttl for negative responses from authoritative name servers



## step 2 – exploring the configuration

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

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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

33



## 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.
          .      2006031201 ; 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
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

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

last update: Dec 2023

34



## 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)

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

35



## 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;
    filter-aaaa-on-v4 yes;
    send-cookie no;
```

disable dnssec

filter AAAA addresses on IPv4 only

allow recursive queries from 192.168.0.0/24

Do not send  
DNS cookies

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

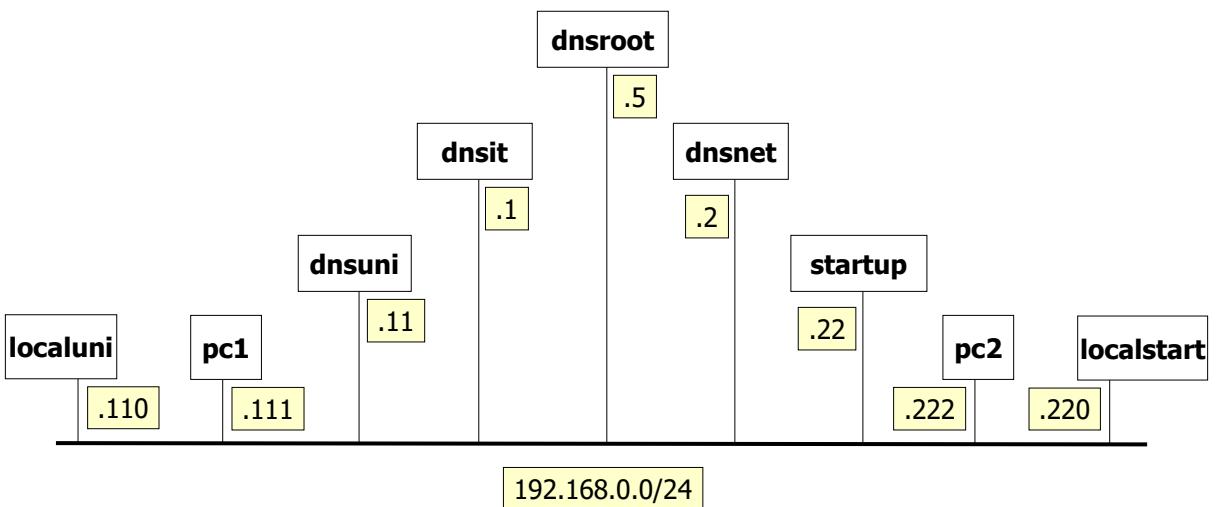
36



# let's start the lab



## step 3 – experiment setting





## 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.

```
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 3 – the sniffer output

Screenshot of Wireshark showing captured DNS traffic. A yellow callout bubble points to the interface list in the top left of the packet list pane.

**Selected packet details:**

```

No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0x7d19 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.111 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0x7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.2 DNS 86 Standard query 0x5ac8 A pc2.startup.net OPT
13 0.008519351 192.168.0.2 192.168.0.110 DNS 125 Standard query response 0x5ac8 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
16 0.009507968 192.168.0.110 192.168.0.22 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 0xecbb 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 0xecbb AAAA pc2.startup.net SOA dnsstart.startup.net

```

**Selected packet bytes:**

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
          ee d6 b8 29 cf ae 92 93 6c 69 91 fc 08 00 45 00 ... )... 11 ..E
          0010 00 3d fa ef 40 00 40 11 bd 92 c0 a8 00 6f c0 a8 ... @ @ ...
          0020 00 6e 9b 9e 00 35 00 29 f5 86 b5 d4 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 ...

```

**Selected packet annotations:**

- Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
- 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: 39838, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xb5d4
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - Response In: 181

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

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

41



## step 3 – the sniffer output filter to only show DNS packets

Screenshot of Wireshark showing captured DNS traffic. A yellow callout bubble points to the interface list in the top left of the packet list pane.

**Selected packet details:**

```

No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0x7d19 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.111 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0x7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.2 DNS 86 Standard query 0x5ac8 A pc2.startup.net OPT
13 0.008519351 192.168.0.2 192.168.0.110 DNS 125 Standard query response 0x5ac8 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
16 0.009507968 192.168.0.110 192.168.0.22 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 0xecbb 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 0xecbb AAAA pc2.startup.net SOA dnsstart.startup.net

```

**Selected packet bytes:**

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
          ee d6 b8 29 cf ae 92 93 6c 69 91 fc 08 00 45 00 ... )... 11 ..E
          0010 00 3d fa ef 40 00 40 11 bd 92 c0 a8 00 6f c0 a8 ... @ @ ...
          0020 00 6e 9b 9e 00 35 00 29 f5 86 b5 d4 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 ...

```

**Selected packet annotations:**

- Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
- 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: 39838, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xb5d4
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - Response In: 181

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

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

42

**step 3 – the sniffer output**

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

**query id**

**query value**

**query type  
(address)**

Screenshot of Wireshark showing DNS traffic. A yellow callout points to the query ID (0xb5d4) in the first packet. Another yellow callout points to the query value (pc2.startup.net) in the second packet. A third yellow callout points to the query type (Address) in the third packet.

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0xd719 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.110 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0xd719 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.22 DNS 86 Standard query 0x722b AAAA pc2.startup.net OPT
13 0.008519351 192.168.0.22 192.168.0.110 DNS 136 Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
16 0.009507968 192.168.0.22 192.168.0.110 DNS 125 Standard query response 0x4bba A pc2.startup.net SOA dnsstart.startup.net
17 0.009914852 192.168.0.22 192.168.0.110 DNS 102 Standard query response 0x4bba A pc2.startup.net A 192.168.0.22 OPT
18 0.010656291 192.168.0.110 192.168.0.111 DNS 130 Standard query response 0xd4 A pc2.startup.net NS start.startup.net A 192.168.0.22
19 0.010932933 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xeccc 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
22 0.012129873 192.168.0.110 192.168.0.111 DNS 125 Standard query response 0xeccc AAAA pc2.startup.net SOA dnsstart.startup.net

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0xd719 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.110 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0xd719 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.22 DNS 86 Standard query 0x722b AAAA pc2.startup.net OPT
13 0.008519351 192.168.0.22 192.168.0.110 DNS 136 Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
16 0.009507968 192.168.0.22 192.168.0.110 DNS 125 Standard query response 0x4bba A pc2.startup.net SOA dnsstart.startup.net
17 0.009914852 192.168.0.22 192.168.0.110 DNS 102 Standard query response 0x4bba A pc2.startup.net A 192.168.0.22 OPT
18 0.010656291 192.168.0.110 192.168.0.111 DNS 130 Standard query response 0xd4 A pc2.startup.net NS start.startup.net A 192.168.0.22
19 0.010932933 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xeccc 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
22 0.012129873 192.168.0.110 192.168.0.111 DNS 125 Standard query response 0xeccc AAAA pc2.startup.net SOA dnsstart.startup.net

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

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

43

**step 3 – the sniffer output**

**request root  
name servers**

**answer with all  
the authoritative  
root name servers**

Screenshot of Wireshark showing DNS traffic. A yellow callout points to the request for root name servers (0xb5d4) in the first packet. Another yellow callout points to the answer from all authoritative root name servers (0x4bba) in the second packet.

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0xd719 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.110 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0xd719 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.22 DNS 86 Standard query 0x722b AAAA pc2.startup.net OPT
13 0.008519351 192.168.0.22 192.168.0.110 DNS 136 Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
16 0.009507968 192.168.0.22 192.168.0.110 DNS 125 Standard query response 0x4bba A pc2.startup.net SOA dnsstart.startup.net
17 0.009914852 192.168.0.22 192.168.0.110 DNS 102 Standard query response 0x4bba A pc2.startup.net A 192.168.0.22 OPT
18 0.010656291 192.168.0.110 192.168.0.111 DNS 130 Standard query response 0xd4 A pc2.startup.net NS start.startup.net A 192.168.0.22
19 0.010932933 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xeccc 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
22 0.012129873 192.168.0.110 192.168.0.111 DNS 125 Standard query response 0xeccc AAAA pc2.startup.net SOA dnsstart.startup.net

```

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface et0
No. Time Source Destination Protocol Length Info
3 0.000433391 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xb5d4 A pc2.startup.net
6 0.003975910 192.168.0.110 192.168.0.5 DNS 86 Standard query 0x8ff1 A pc2.startup.net OPT
7 0.004044955 192.168.0.110 192.168.0.5 DNS 70 Standard query 0xd719 NS <Root> OPT
8 0.004896721 192.168.0.5 192.168.0.110 DNS 123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9 0.005024653 192.168.0.5 192.168.0.110 DNS 110 Standard query response 0xd719 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
12 0.006382260 192.168.0.110 192.168.0.22 DNS 86 Standard query 0x722b AAAA pc2.startup.net OPT
13 0.008519351 192.168.0.22 192.168.0.110 DNS 136 Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
16 0.009507968 192.168.0.22 192.168.0.110 DNS 125 Standard query response 0x4bba A pc2.startup.net SOA dnsstart.startup.net
17 0.009914852 192.168.0.22 192.168.0.110 DNS 102 Standard query response 0x4bba A pc2.startup.net A 192.168.0.22 OPT
18 0.010656291 192.168.0.110 192.168.0.111 DNS 130 Standard query response 0xd4 A pc2.startup.net NS start.startup.net A 192.168.0.22
19 0.010932933 192.168.0.111 192.168.0.110 DNS 75 Standard query 0xeccc 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
22 0.012129873 192.168.0.110 192.168.0.111 DNS 125 Standard query response 0xeccc AAAA pc2.startup.net SOA dnsstart.startup.net

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

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

44

**step 3 – the sniffer output**

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

**dnsnet.net address is**  
**192.168.0.2**

No.	Time	Source	Destination	Protocol	Length Info
3	0.000433391	192.168.0.110	192.168.0.110	DNS	75 Standard query 0xb5d4 A pc2.startup.net
6	0.003975918	192.168.0.110	192.168.0.5	DNS	86 Standard query 0x8ff1 A pc2.startup.net OPT
7	0.004044955	192.168.0.110	192.168.0.5	DNS	70 Standard query 0xd19 NS <Root> OPT
8	0.004896721	192.168.0.5	192.168.0.110	DNS	123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
9	0.005024653	192.168.0.5	192.168.0.110	DNS	110 Standard query 0xb5d4 A pc2.startup.net OPT
10	2.011471405	192.168.0.110	192.168.0.22	DNS	86 Standard query 0x5ac8 A 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 dnstart.startup.net OPT

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 1  
Queries  
Additional records  
- <Root> type OPT  
  Name: <Root>  
  Type: OPT (41)  
  UDP payload size: 512  
  Higher bits in extended RCODE: 0x00  
  EDNS0 version: 0  
- Z: 0x8000  
  1... = DO bit: Accepts DNSSEC security RRs  
  .000 0000 0000 0000 = Reserved: 0x0000

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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ] last update: Dec 2023

45

**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**

No.	Time	Source	Destination	Protocol	Length Info
8	0.004896721	192.168.0.110	192.168.0.110	DNS	75 Standard query 0xb5d4 A pc2.startup.net
9	0.005024653	192.168.0.5	192.168.0.110	DNS	86 Standard query 0x8ff1 A pc2.startup.net OPT
10	12.006382265	192.168.0.2	192.168.0.110	DNS	123 Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
13	0.008519351	192.168.0.2	192.168.0.110	DNS	110 Standard query response 0xd19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
16	0.009507968	192.168.0.110	192.168.0.22	DNS	86 Standard query 0xb5d4 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	192.168.0.17	192.168.0.110	DNS	86 Standard query 0xb5d4 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
19	0.010932933	192.168.0.1	192.168.0.110	DNS	102 Standard query response 0xb5d4 A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
20	0.011471405	192.168.0.1	192.168.0.110	DNS	102 Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net OPT
21	0.011875739	192.168.0.22	192.168.0.110	DNS	125 Standard query response 0xeccb AAAA pc2.startup.net SOA dnstart.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 dnstart.startup.net OPT

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 1  
Queries  
Additional records  
- <Root> type OPT  
  Name: <Root>  
  Type: OPT (41)  
  UDP payload size: 512  
  Higher bits in extended RCODE: 0x00  
  EDNS0 version: 0  
- Z: 0x8000  
  1... = DO bit: Accepts DNSSEC security RRs  
  .000 0000 0000 0000 = Reserved: 0x0000

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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ] last update: Dec 2023

46



## 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**

No.	Time	Source	Destination	Protocol	Length	Info
9	0.005024653	192.168.0.110	192.168.0.110	DNS	75	Standard query 0xb5d4 A pc2.startup.net
10	0.005382260	192.168.0.110	192.168.0.2	DNS	86	Standard query 0x8ff1 A pc2.startup.net OPT
11	0.008519351	192.168.0.2	192.168.0.110	DNS	70	Standard query 0xd7d19 NS <Root> OPT
12	0.009507968	192.168.0.2	192.168.0.222	DNS	123	Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
13	0.009514852	192.168.0.222	192.168.0.110	DNS	110	Standard query response 0xd7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
14	0.009507968	192.168.0.222	192.168.0.222	DNS	86	Standard query 0x4bba A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
15	0.009514852	192.168.0.222	192.168.0.222	DNS	102	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 OPT
16	0.009507968	192.168.0.222	192.168.0.110	DNS	130	Standard query response 0xb5d4 A pc2.startup.net OPT
17	0.009514852	192.168.0.222	192.168.0.110	DNS	125	Standard query response 0x5ac8 A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22
18	0.010656291	192.168.0.110	192.168.0.111	DNS	75	Standard query 0x4bba 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	192.168.0.111	DNS	75	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
20	0.011471495	192.168.0.111	192.168.0.111	DNS	75	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 NS dnsstart.startup.net A 192.168.0.22
21	0.011875739	192.168.0.111	192.168.0.111	DNS	136	Standard query response 0x722b AAAA pc2.startup.net SOA dnsstart.startup.net OPT
22	0.012129873	192.168.0.111	192.168.0.111	DNS	125	Standard query response 0xeccb AAAA pc2.startup.net SOA dnsstart.startup.net

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 1  
Queries  
- Additional records  
- <Root> type OPT  
  Name: <Root>  
  Type: OPT (41)  
  UDP payload size: 512  
  Higher bits in extended RCODE: 0x00  
  EDNS0 version: 0  
- Z: 0x8000  
  1... .... .... .... = DO bit: Accepts DNSSEC security RRs  
  .... 0000 0000 0000 0000 = Reserved: 0x0000

Packets: 40 (Displayed: 14 (35.0%))

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

47



## step 3 – the sniffer output

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

No.	Time	Source	Destination	Protocol	Length	Info
13	0.008519351	192.168.0.110	192.168.0.110	DNS	75	Standard query 0xb5d4 A pc2.startup.net
14	0.008507968	192.168.0.110	192.168.0.222	DNS	86	Standard query 0x8ff1 A pc2.startup.net OPT
15	0.009514852	192.168.0.222	192.168.0.110	DNS	123	Standard query response 0x8ff1 A pc2.startup.net NS dnsnet.net A 192.168.0.2 OPT
16	0.009507968	192.168.0.222	192.168.0.222	DNS	110	Standard query response 0xd7d19 NS <Root> NS ROOT-SERVER A 192.168.0.5 OPT
17	0.009514852	192.168.0.222	192.168.0.222	DNS	86	Standard query 0x4bba A pc2.startup.net NS dnsstart.startup.net A 192.168.0.22 OPT
18	0.009514852	192.168.0.222	192.168.0.111	DNS	130	Standard query response 0x4bba A pc2.startup.net A 192.168.0.222 OPT
19	0.010932933	192.168.0.111	192.168.0.110	DNS	75	Standard query 0xeccb AAAA pc2.startup.net
20	0.011471495	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  
- 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

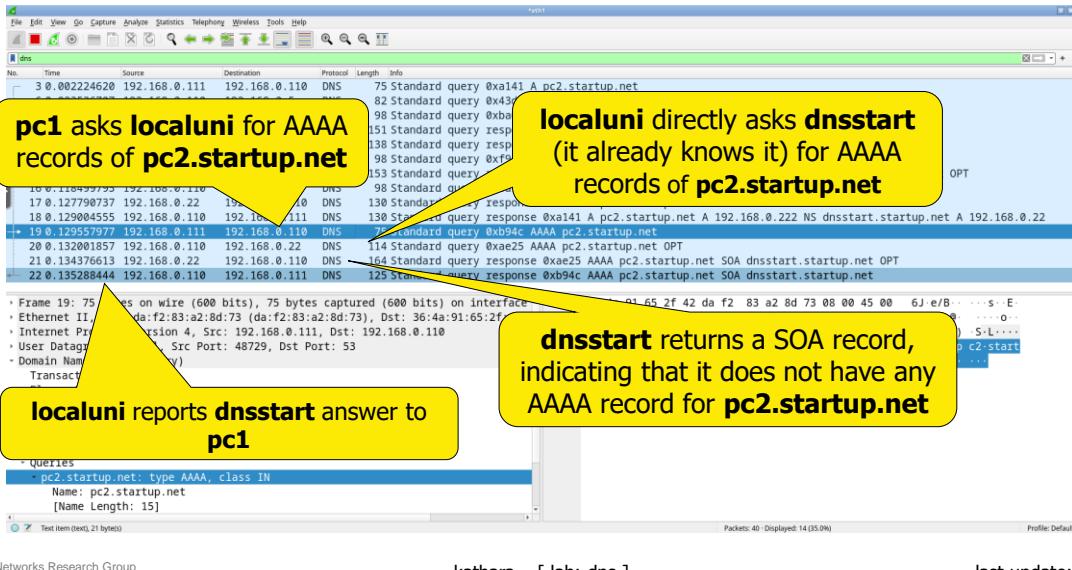
Packets: 40 (Displayed: 14 (35.0%))

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

48



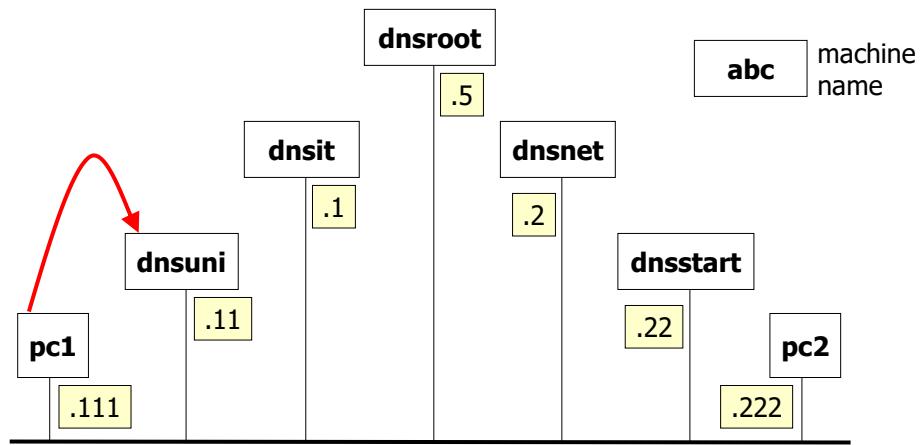
## step 3 – the sniffer output



49



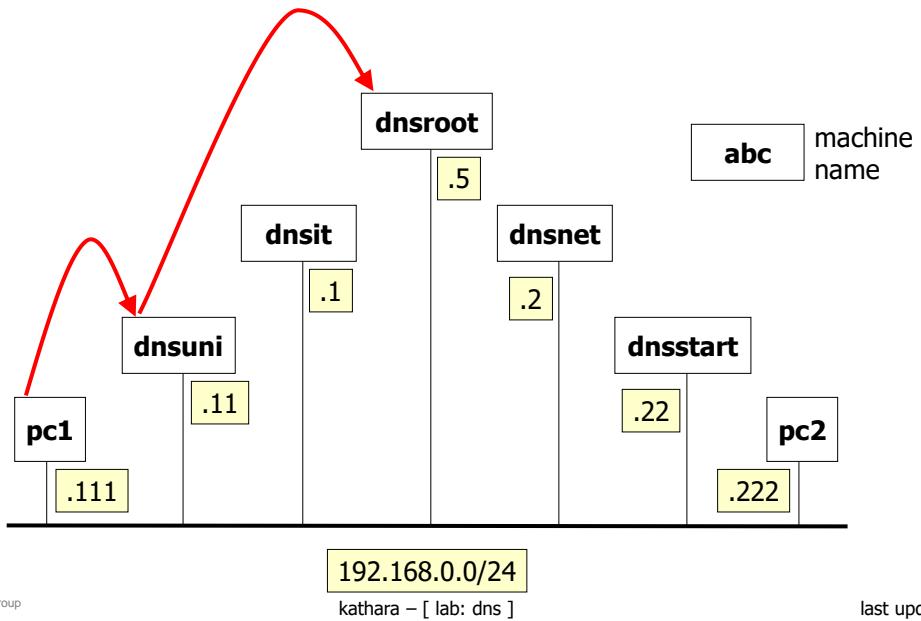
## step 3 – exchanged messages



50



## step 3 – exchanged messages



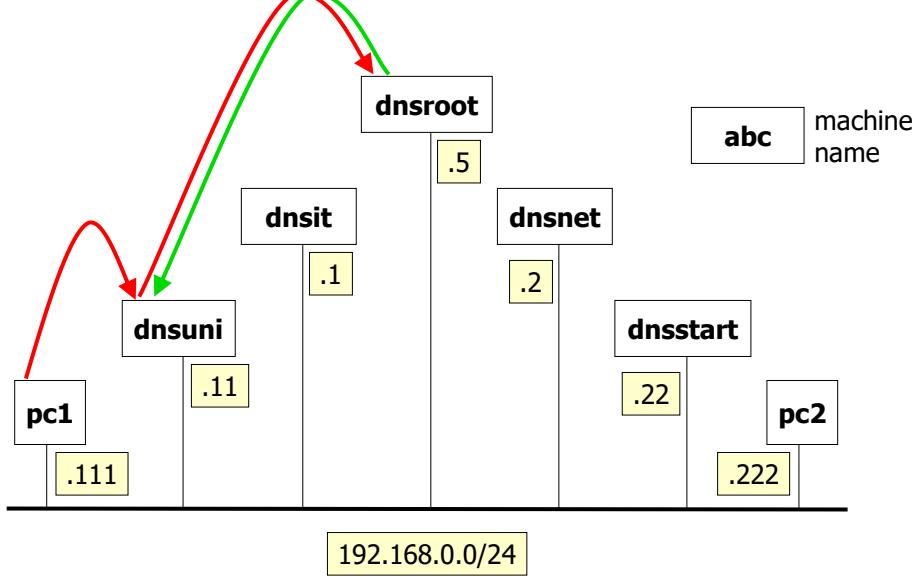
51

© Computer Networks Research Group  
Roma Tre University

last update: Dec 2023

52

## step 3 – exchanged messages

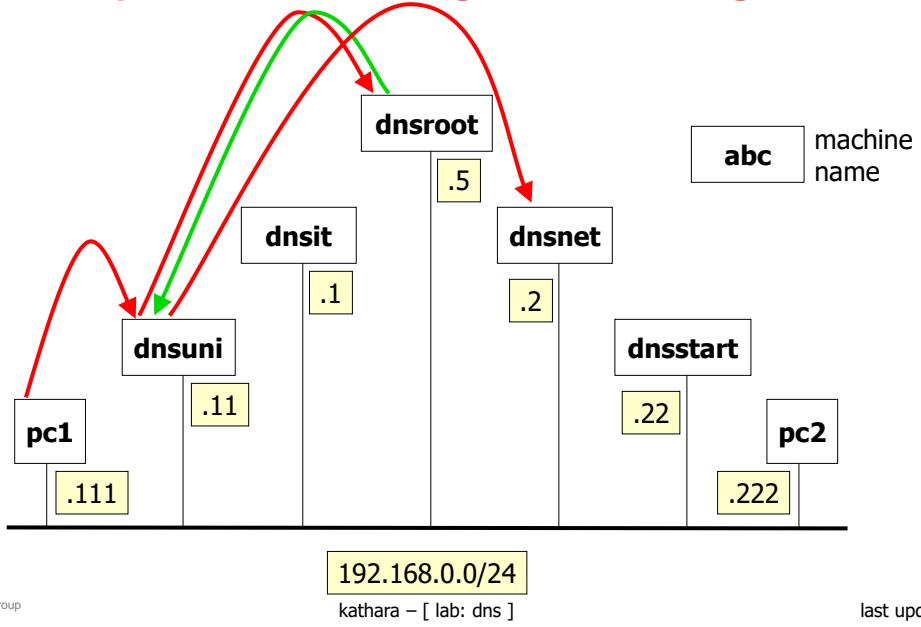


last update: Dec 2023

26



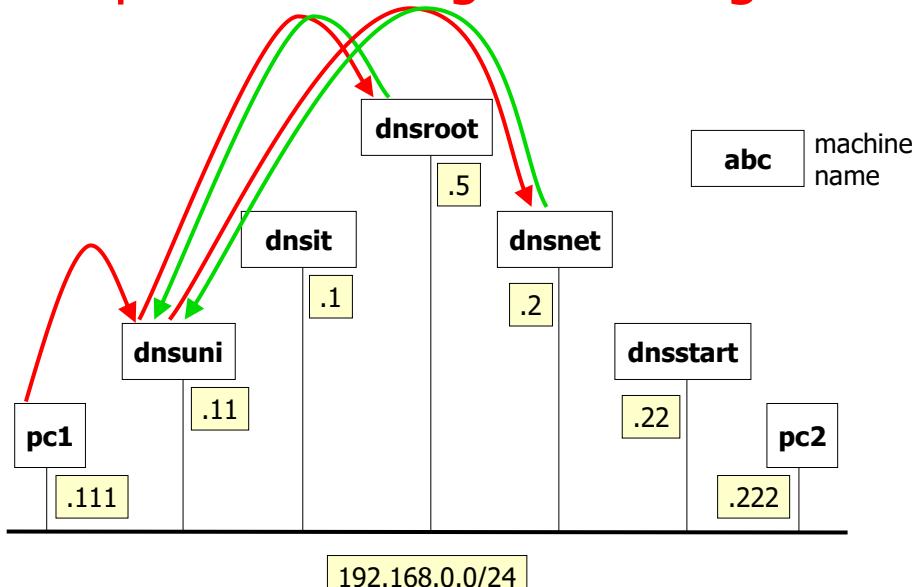
## step 3 – exchanged messages



53



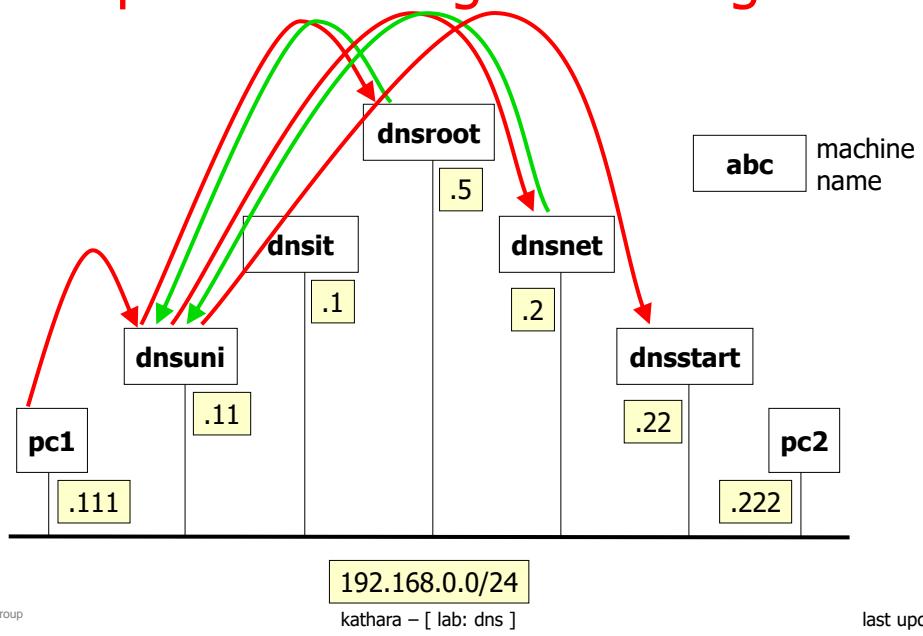
## step 3 – exchanged messages



54



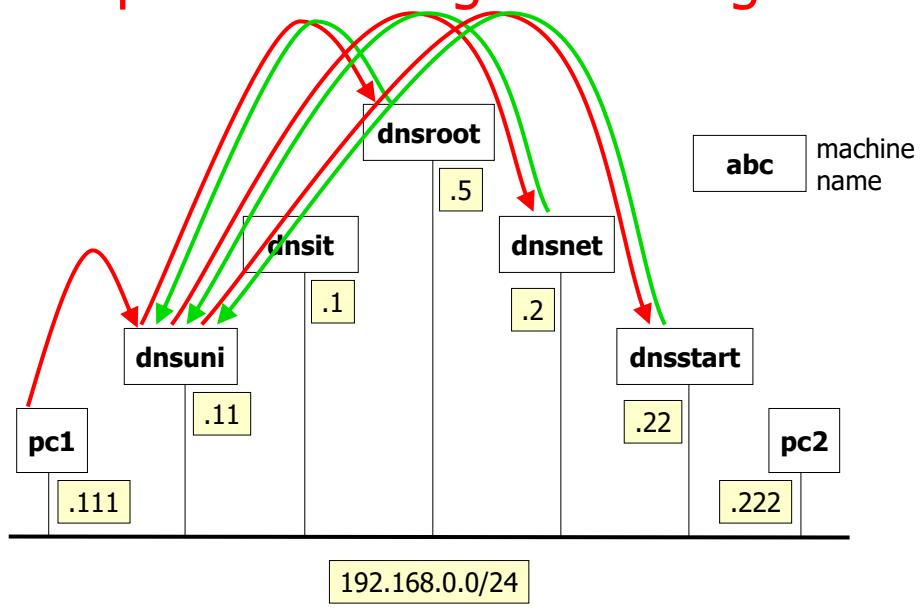
## step 3 – exchanged messages



55



## step 3 – exchanged messages

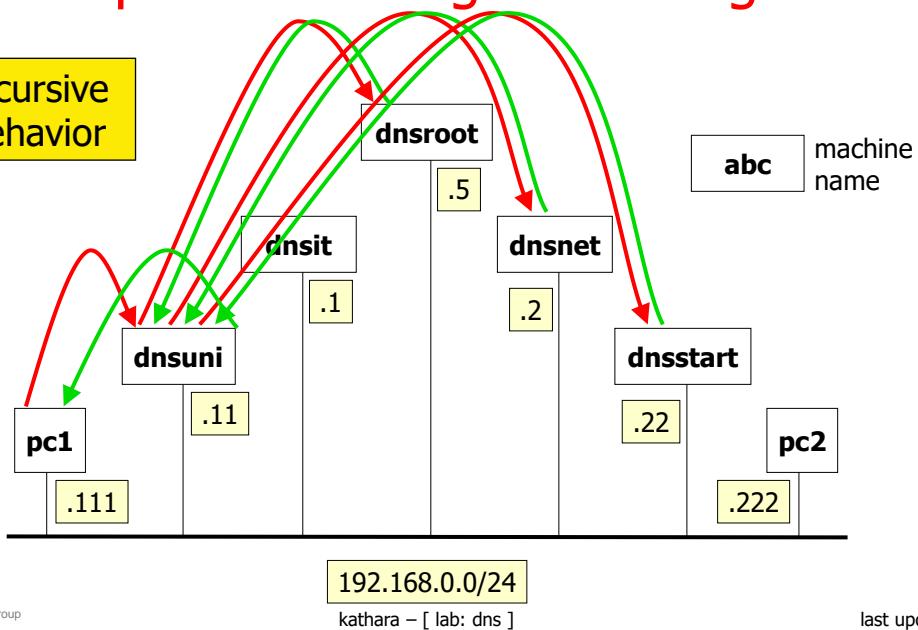


56



## step 3 – exchanged messages

recursive behavior



© Computer Networks Research Group  
Roma Tre University

192.168.0.0/24

kathara – [ lab: dns ]

last update: Dec 2023

57



## 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
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

58



## step 4 – repeating the experiment

Screenshot of Wireshark showing DNS traffic. A yellow callout box points to the interface:

the name server cache helps reducing traffic

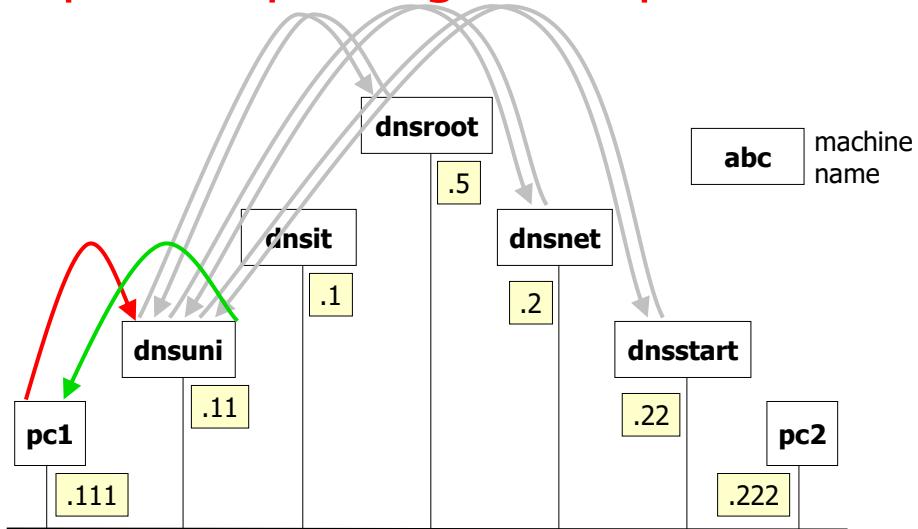
Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth1  
Ethernet II, Src: 92:93:6c:69:91:fc (92:93:6c:69:91:fc), Dst: ee:d6:b8:29:cf:ae (ee:d6:b8:29:cf:ae)  
Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.110  
User Datagram Protocol, Src Port: 35784, Dst 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: 2]

© Computer Networks Research Group Roma Tre University kathara – [ lab: dns ] last update: Dec 2023

59



## step 4 – repeating the experiment



© Computer Networks Research Group  
Roma Tre University

192.168.0.0/24

kathara – [ lab: dns ]

last update: Dec 2023

60



## 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**



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

Screenshot of Wireshark showing DNS traffic. The timeline shows multiple DNS queries from 192.168.0.110 to 192.168.0.111. A yellow callout points to the first few queries. The packet details pane shows the raw hex and ASCII data for each packet.

© Computer Networks Research Group  
Roma Tre University

kathara - [ lab: dns ] last update: Dec 2023

63

**step 6 – non-existent target**



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

Screenshot of Wireshark showing DNS traffic. The timeline shows multiple DNS queries from 192.168.0.110 to 192.168.0.111. A yellow callout points to the first few queries. The packet details pane shows the raw hex and ASCII data for each packet.

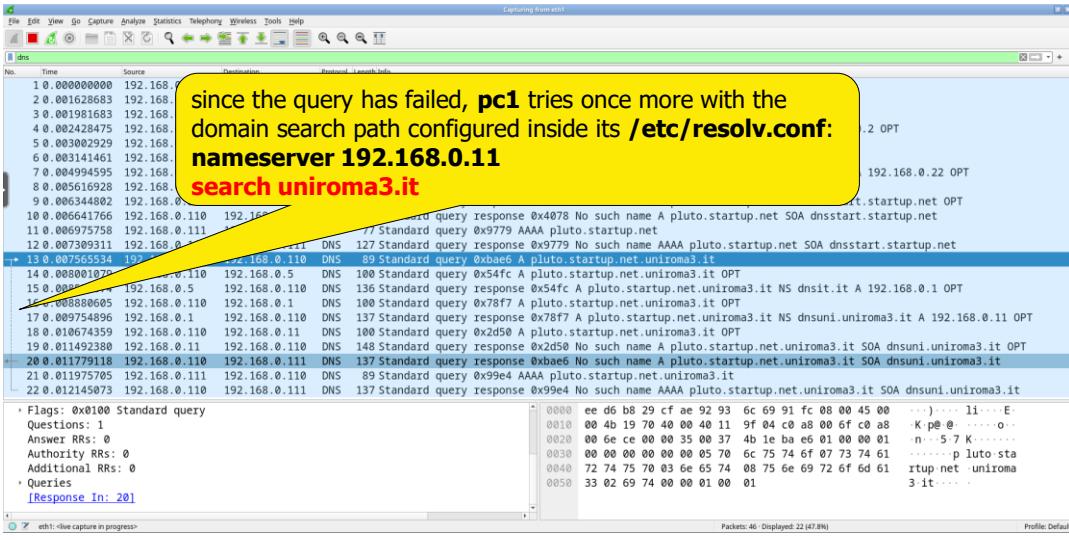
© Computer Networks Research Group  
Roma Tre University

kathara - [ lab: dns ] last update: Dec 2023

64



## step 6 – non-existent target



© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

65



## 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
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

66



**step 6 – ping non-existent target**

the name server negative cache has stored the negative answer

No.	Time	Source	Destination	Protocol	Length	Info
+ 1	10.000000000	192.168.0.111	192.168.0.110	DNS	77	Standard query A pluto.startup.net
+ 2	0.000630274	192.168.0.110	192.168.0.111	DNS	127	Standard query response 0xfe4 No such name A pluto.startup.net SOA dnsstart.startup.net
+ 3	0.000812191	192.168.0.111	192.168.0.110	DNS	77	Standard query 0x9ae5 AAAA pluto.startup.net
+ 4	0.001195322	192.168.0.110	192.168.0.111	DNS	127	Standard query response 0x9ae5 No such name AAAA pluto.startup.net SOA dnsstart.startup.net
+ 5	0.001788267	192.168.0.111	192.168.0.110	DNS	89	Standard query 0xaceaf A pluto.startup.net.uniroma3.it
+ 6	0.002311232	192.168.0.110	192.168.0.111	DNS	137	Standard query response 0xaceaf No such name A pluto.startup.net.uniroma3.it SOA dnsuni.uniroma3.it
+ 7	0.002651008	192.168.0.111	192.168.0.110	DNS	89	Standard query 0x67cd AAAA pluto.startup.net.uniroma3.it
+ 8	0.003023875	192.168.0.110	192.168.0.111	DNS	137	Standard query response 0x67cd No such name AAAA pluto.startup.net.uniroma3.it SOA dnsuni.uniroma3.it

as before, **pc1** tries once more with the domain search path configured inside its **/etc/resolv.conf**

Questions: 1	0000	92 93 6c 69 91 fc ee d6	b8 29 cf ae 08 00 45 00	li .. ) .. E
Answer RRS: 0	0010	00 71 c3 57 00 00 40 11	b7 f7 c0 a8 00 60 c0 a8	q=W .. ) .. n
Authority RRS: 1	0020	6f 00 35 b7 1c 00 5d 70	b2 c2 ff e4 81 83 00 01	o 5 .. ) p ..
Additional RRS: 0	0030	00 00 00 01 00 00 85 70	6c 75 74 67 07 73 74 61	p .. ) puto-sta
• Queries	0040	72 74 75 70 03 6e 65 74	00 00 01 00 01 00 12 00	rtp-net ..
- Authoritative nameservers	0050	00 00 01 00 00 28 33 00	26 08 64 66 73 74 61	(3 .. ) .. dnst-a
• startup.net type 50A, class IN, mname dnsstart.startup.net	0060	72 74 c8 d2 04 72 6f 4f	74 c8 2f 77 91 9b 61 00	rt .. )oo t .. w-a
Normal resolution	0070	00 00 1c 00 00 38 40 00	36 ee 80 00 00 00 00 0f	.. ) .. 80 6 ..
• Test item (next, 50 bytes)			Packets 12 - Displayed 8 (66.7%)	Profile: Default

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

7



## step 7 – advanced queries

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

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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

68



## 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 pc2.startup.net
; <>> DiG 9.18.19-1~deb12u1-Debian <>> pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: b4c95f2012cf8905d705a97c657b10f314be1a5abe3ec74d (good)
;; QUESTION SECTION:
;pc2.startup.net.           IN      A
;;
;; ANSWER SECTION:
pc2.startup.net.      60000   IN      A      192.168.0.222
;;
;; AUTHORITY SECTION:
startup.net.          59173   IN      NS     dnsstart.startup.net.
;;
;; ADDITIONAL SECTION:
dnsstart.startup.net. 59173   IN      A      192.168.0.22
;;
;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:28:03 UTC 2023
;; MSG SIZE rcvd: 127
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

69



## step 7 – advanced queries

these sections correspond to those contained in DNS packets

```
pc1
root@pc1:/# dig pc2.startup.net
; <>> DiG 9.18.19-1~deb12u1-Debian <>> pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: b4c95f2012cf8905d705a97c657b10f314be1a5abe3ec74d (good)
;; QUESTION SECTION:
;pc2.startup.net.           IN      A
;;
;; ANSWER SECTION:
pc2.startup.net.      60000   IN      A      192.168.0.222
;;
;; AUTHORITY SECTION:
startup.net.          59173   IN      NS     dnsstart.startup.net.
;;
;; ADDITIONAL SECTION:
dnsstart.startup.net. 59173   IN      A      192.168.0.22
;;
;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:28:03 UTC 2023
;; MSG SIZE rcvd: 127
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

70



## step 7 – advanced queries

records being searched  
(class: IN, type: A ⇒  
address records)

a dns message never  
contains more than one  
question section

```
pc1
root@pc1:/# dig pc2.startup.net
; <>> DiG 9.18.19-1~deb12u1-Debian <>> pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: b4c95f2012cf8905d705a97c657b10f314be1a5abe3ec74d (good)
;; QUESTION SECTION:
;pc2.startup.net.           IN      A

;; ANSWER SECTION:
pc2.startup.net.      60000   IN      A      192.168.0.222

;; AUTHORITY SECTION:
startup.net.          59173   IN      NS     dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59173   IN      A      192.168.0.22

;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:28:03 UTC 2023
;; MSG SIZE rcvd: 127
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

71



## step 7 – advanced queries

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

```
pc1
root@pc1:/# dig pc2.startup.net
; <>> DiG 9.18.19-1~deb12u1-Debian <>> pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: b4c95f2012cf8905d705a97c657b10f314be1a5abe3ec74d (good)
;; QUESTION SECTION:
;pc2.startup.net.           IN      A

;; ANSWER SECTION:
pc2.startup.net.      60000   IN      A      192.168.0.222

;; AUTHORITY SECTION:
dnsstart.startup.net. 59173   IN      NS     dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59173   IN      A      192.168.0.22

;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:28:03 UTC 2023
;; MSG SIZE rcvd: 127
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

72



## step 7 – advanced queries

```
pc1
root@pc1:/# dig pc2.startup.net
; <>> DiG 9.18.19-1~deb12u1-Debian <>> pc2.startup.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b4c95f2012cf8905d705a97c657b10f314be1a5abe3ec74d (good)
; QUESTION SECTION:
;pc2.startup.net.           IN      A

;; ANSWER SECTION:
pc2.startup.net.    60000   IN      A      192.168.0.222

;; AUTHORITY SECTION:
startup.net.        59173   IN      NS     dnsstart.startup.net.

;; ADDITIONAL SECTION:
dnsstart.startup.net. 59173   IN      A      192.168.0.22

;; Query time: 0 msec
;; SERVER: 192.168.0.110#53(192.168.0.110) (UDP)
;; WHEN: Thu Dec 14 14:28:03 UTC 2023
;; MSG SIZE  rcvd: 127
```

records describing authoritative name servers are returned here

additional records are returned here

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

73



## 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

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

74



## 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

.
.
.
; (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
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

77



## 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

.
.
.
; (1 server found)
; 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
```

© Computer Networks Research Group  
Roma Tre University

kathara – [ lab: dns ]

last update: Dec 2023

78