

Lab - DNS (Domain Name System)

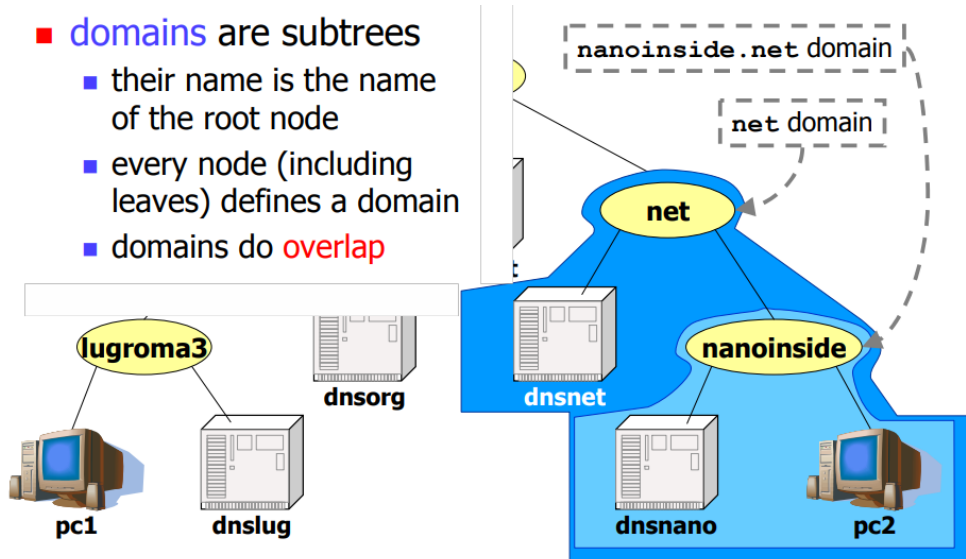
Ecrivez un compte rendu des résultats de votre expérimentation, et répondez aux questions.

http://wiki.netkit.org/netkit-labs/netkit-labs_application-level/netkit-lab_dns/netkit-lab_dns.pdf

http://wiki.netkit.org/netkit-labs/netkit-labs_application-level/netkit-lab_dns/netkit-lab_dns.tar.gz

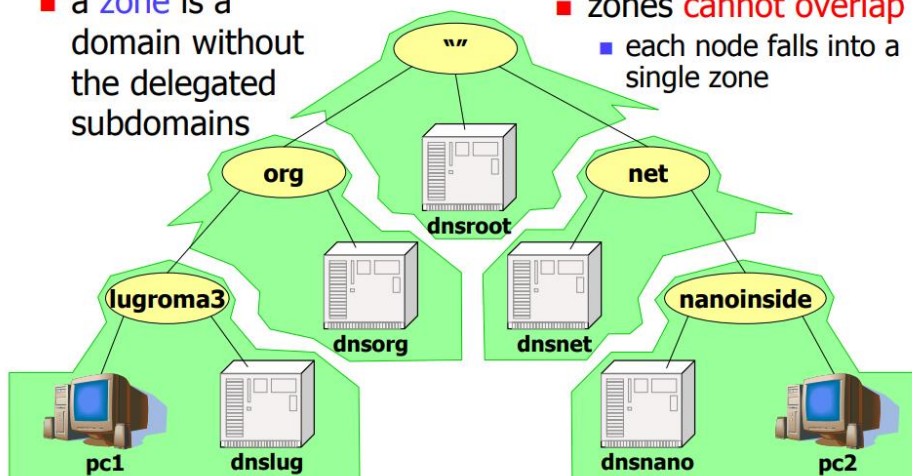
Domaines dans notre topologie

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

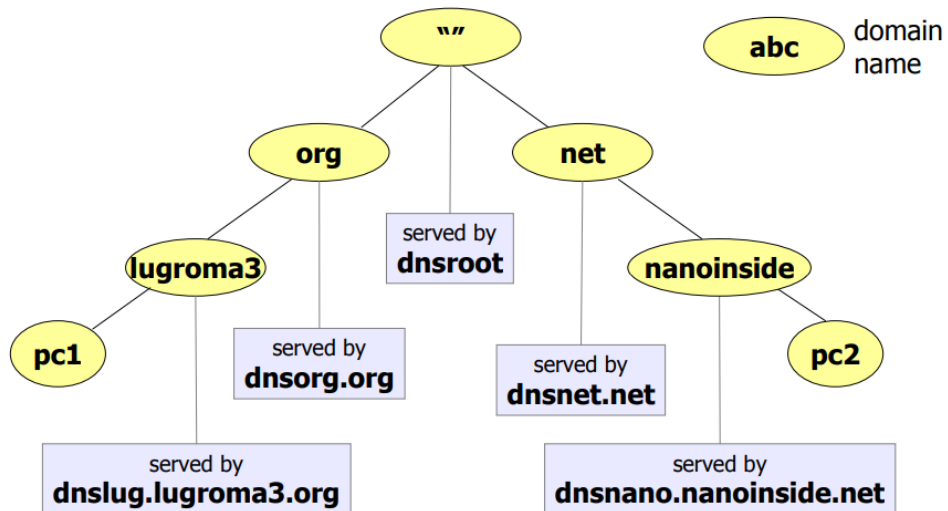
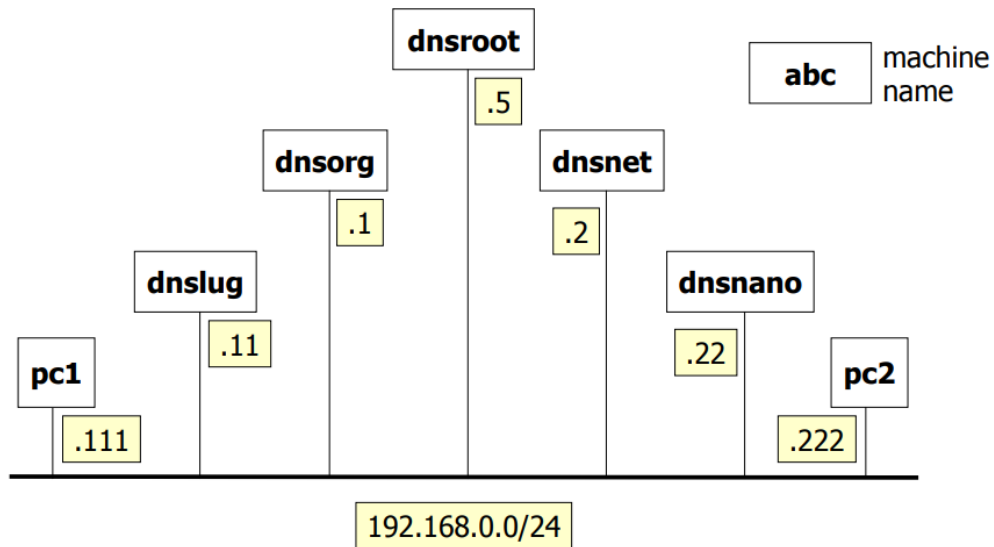


Zones dans notre topologie

- a **zone** is a domain without the delegated subdomains
- **zones cannot overlap**
 - each node falls into a single zone



Topologie du Lab



Step 2 – démarrer le lab

Comme d'habitude, pour démarrer le lab :

```
cd netkit-lab_dns lab_dns
```

```
lstart
```

Explorer la configuration des 2 PCs à l'aide de la commande suivante : `cat /etc/resolv.conf`

Q1 : Quel est le « default name server » pour pc1 et pc2 ?

Explorer maintenant la configuration des *name servers*, en particulier en *dnslug* à l'aide de la commande suivante : `cat /etc/bind/named.conf`

Q2 : dans quel fichier peut-on trouver les informations concernant le *root name server* (zone ".") ?

Qui est le *primary master* de la zone `lugroma3.org` ?

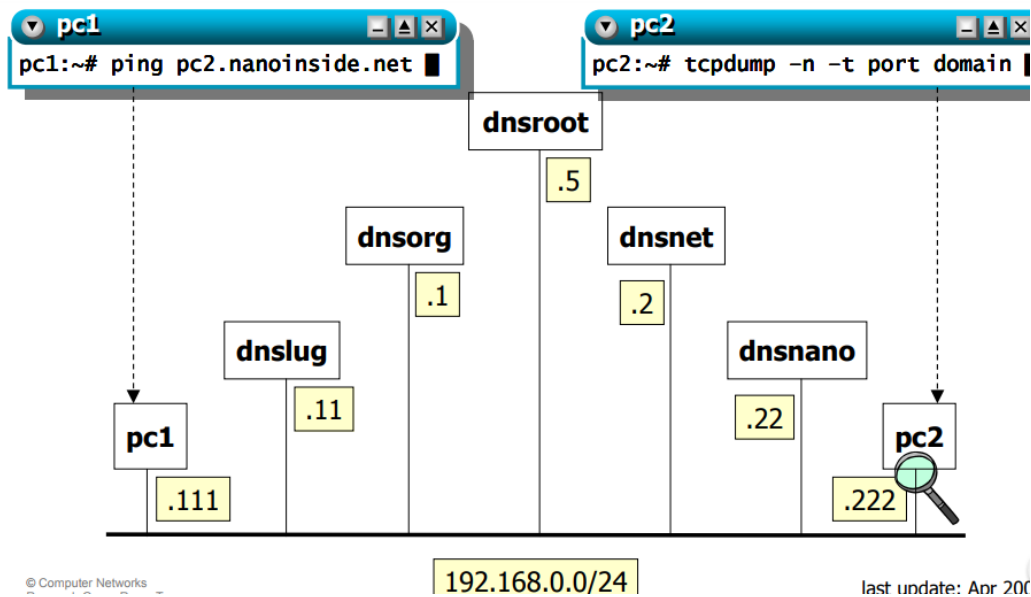
Toujours dans *dnslug*, examinez le contenu du fichier `/etc/bind/db.root`

Et aussi le contenu du fichier `/etc/bind/db.org.lugroma3`

```
dnslug:~# cat /etc/bind/db.org.lugroma3
$TTL      60000
@         IN      SOA     dnslug.lugroma3.org.
root.dnslug.lugroma3.org. (
                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

Step3 - Expérimentation



Tout d'abord on active la commande `tcpdump -n -t port domain` dans **pc2**

Ensuite on fait partir le ping dans **pc1** ping pc2.nanoinside.net

```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
```

Les résultats de la capture sont les suivants :

```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
```

pc2 query answer

```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.5.53 > 192.168.0.11.3073:
    18164 0/1/2 (84)
```

the root server (192.168.0.5) answers with:

- 0 answers
- 1 authority (=name server) record (dnsnet.net)
- 2 additional records (dnsnet.net's IP address 192.168.0.2, and an OPT record)

© Computer Networks

pc2 query answer

```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.5.53 > 192.168.0.11.3073:
    18164 0/1/2 (84)
IP 192.168.0.11.3073 > 192.168.0.2.53:
    19071 [1au] A? pc2.nanoinside.net. (47)
```

the query carries an additional OPT record

dnslug.lugroma3.org
(192.168.0.11)
asks dnsnet.net
(192.168.0.2)

pc2 query answer

```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.5.53 > 192.168.0.11.3073:
    18164 0/1/2 (84)
IP 192.168.0.11.3073 > 192.168.0.2.53:
    19071 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.2.53 > 192.168.0.11.3073:
    19071 0/1/2 (85)
```

dnsnet.net (192.168.0.2) answers with:

- 0 answers
- 1 authority (=name server) record (dnsnano.nanoinside.net)
- 2 additional records (dnsnano.nanoinside.net's IP address 192.168.0.22, and an OPT record)

pc2 query answer

```

pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.5.53 > 192.168.0.11.3073:
    18164 0/1/2 (84)
IP 192.168.0.11.3073 > 192.168.0.2.53:
    19071 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.2.53 > 192.168.0.11.3073:
    19071 0/1/2 (85)
IP 192.168.0.11.3073 > 192.168.0.22.53:
    64854 [1au] A? pc2.nanoinside.net. (47)

```

the query carries an additional OPT record

dnslug.lugroma3.org
 (192.168.0.11)
 asks dnsnano.nanoinside.net
 (192.168.0.22)

pc2 query answer

```

pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
    29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53:
    18164 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.5.53 > 192.168.0.11.3073:
    18164 0/1/2 (84)
IP 192.168.0.11.3073 > 192.168.0.2.53:
    19071 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.2.53 > 192.168.0.11.3073:
    19071 0/1/2 (85)
IP 192.168.0.11.3073 > 192.168.0.22.53:
    64854 [1au] A? pc2.nanoinside.net. (47)
IP 192.168.0.22.53 > 192.168.0.11.3073:
    64854* 1/1/2 A 192.168.0.222 (101)

```

dnsnano.nanoinside.net (192.168.0.22) answers with:

- 1 answer (pc2.nanoinside.net's IP address 192.168.0.222)
- 1 authority (=name server) record (dnsnano.nanoinside.net)
- 2 additional records (dnsnano.nanoinside.net's IP address 192.168.0.22, and an OPT record)

```

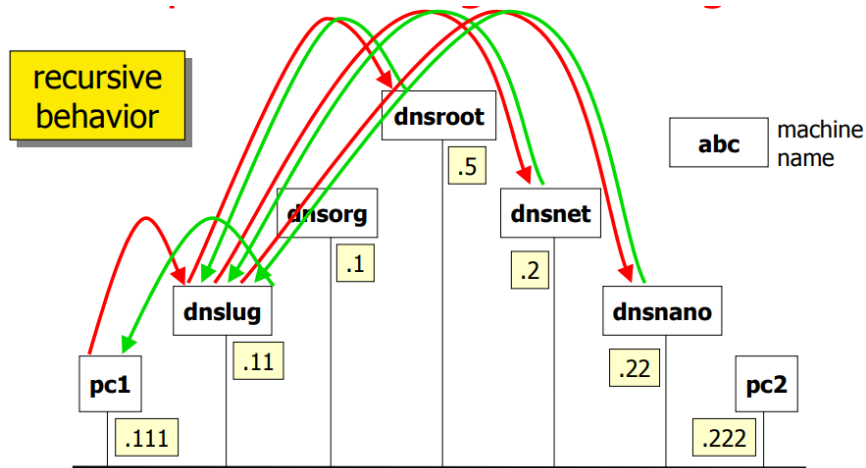
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full
listening on eth0, link-type EN10MB (Ethernet)
IP 192.168.0.111.3072 > 192.168.0.11.53: 29753+ A
IP 192.168.0.11.3073 > 192.168.0.5.53: 18164 [1]
IP 192.168.0.5.53 > 192.168.0.11.3073: 18164 0/
IP 192.168.0.11.3073 > 192.168.0.2.53: 19071 [1]
IP 192.168.0.2.53 > 192.168.0.11.3073: 19071 0/
IP 192.168.0.11.3073 > 192.168.0.22.53: 64854 [1au] A
IP 192.168.0.22.53 > 192.168.0.11.3073: 64854* 1/1/2
IP 192.168.0.11.53 > 192.168.0.111.3072: 29753 1/1/1 (108)

```

dnslug.lugroma3.org (192.168.0.11) answers with:

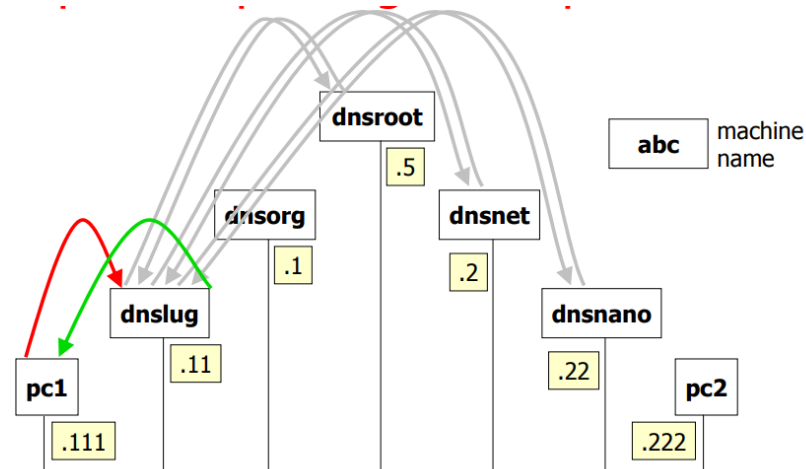
- 1 answer (pc2.nanoinside.net's IP address 192.168.0.222)
- 1 authority (=name server) record (dnsnano.nanoinside.net)
- 1 additional record (dnsnano.nanoinside.net's IP address 192.168.0.22)

Le comportement est récuratif : voici les messages échangés



Step 4 – Expérimentation

Répétez la même expérimentation (cette fois le *caching* réduit le nombre de messages)



Sep 5 – redemarrer le name server

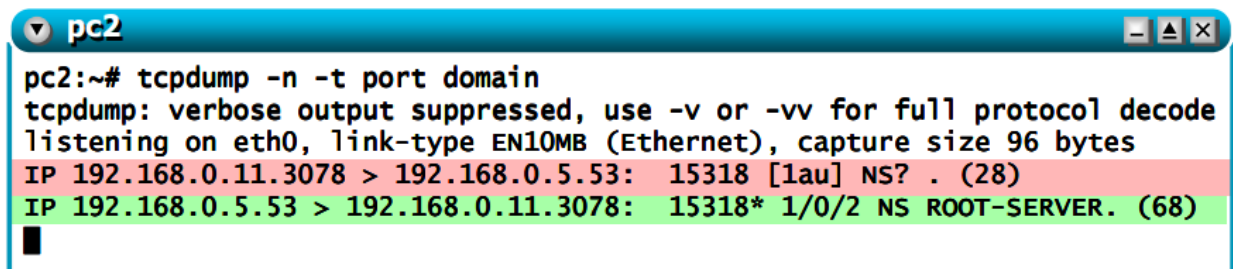
Le redemarrage permet de vider les caches. Une nouvelle query entrainera donc toutes les queries récursives comme vu précédemment.

Laissez tcpdump actif sur pc2.

Ensuite, la commande à utiliser est la suivante (dans *dnslug*) :

```
/etc/init.d/bind restart
```

Le name server, au startup, va vérifier la root server configuration



```
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.11.3078 > 192.168.0.5.53: 15318 [1au] NS? . (28)
IP 192.168.0.5.53 > 192.168.0.11.3078: 15318* 1/0/2 NS ROOT-SERVER. (68)
```

Step 6 – target non-existent

En pc1, utilisez maintenant la commande suivante (laissez tcpdump toujours actif en pc2 avant de lancer le ping) :

```
ping pluto.nanoinside.net
```

Q3 : observez la capture tcpdump en pc2 et comparez-la à celle obtenu auparavant, avec le ping pc2.nanoinside.net

Q4 : ensuite, répétez la même expérimentation (ping vers *pluto.nanoinside.net*) et à l'aide de tcpdump en pc2 vérifiez les messages échangés (et le fait que le réponses soit maintenant déjà en cache).

Step 7 – Queries avancés

Nous utilisons maintenant la commande *dig* qui donne de réponses détaillées.

```
En pc1 : dig pc2.nanoinside.net
```

Observez le résultat :


```

pc1:~# dig pc2.nanoinside.net

; <<> DiG 9.3.1 <<> pc2.nanoinside.net
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 25601
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
pc2.nanoinside.net.                IN      A

;; ANSWER SECTION:
pc2.nanoinside.net.                47861   IN      A

;; AUTHORITY SECTION:
nanoinside.net.                    47861   IN      NS

;; ADDITIONAL SECTION:
dnsnano.nanoinside.net.            48956   IN      A      192.168.0.22

;; Query time: 129 msec
;; SERVER: 192.168.0.11#53(192.168.0.11)

```

Step 8 – query iterative

Il s'agit donc d'une query iterative, et non pas recursive.

Utilisez en pc1 la commande

```
dig +noquestion +noadditional +norecurse pc2.nanoinside.net
```

Observez le résultat.

Il est aussi possible de contacter un server spécifique, par exemple dnsroot :

```
dig +noquestion +noadditional +norecurse @192.168.0.5 pc2.nanoinside.net
```

Ou dnsnet.net

```
dig +noquestion +noadditional +norecurse @192.168.0.2 pc2.nanoinside.net
```

Ou dnsnano.nanoinside.net

```
dig +noquestion +noadditional +norecurse @192.168.0.22 pc2.nanoinside.net
```