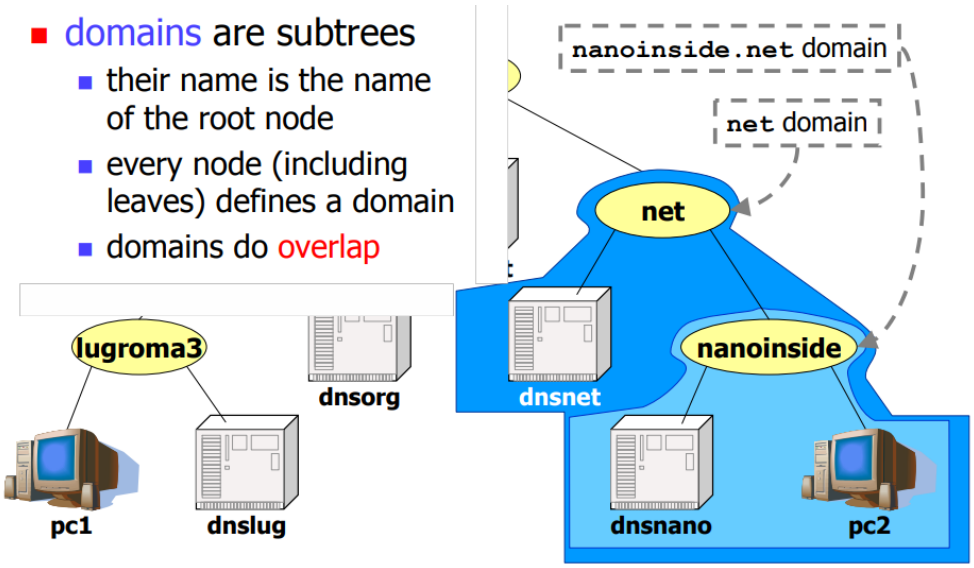
Lab – DNS (Domain Name System)

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

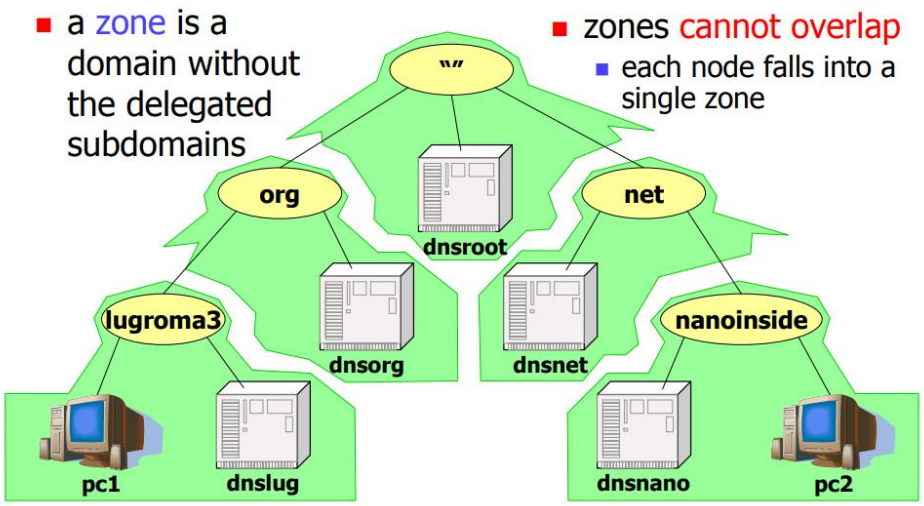
http://wiki.netkit.org/netkit-labs/netkit-labs_application-level/netkit-lab_dns/netkit-lab_dns.pdf

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

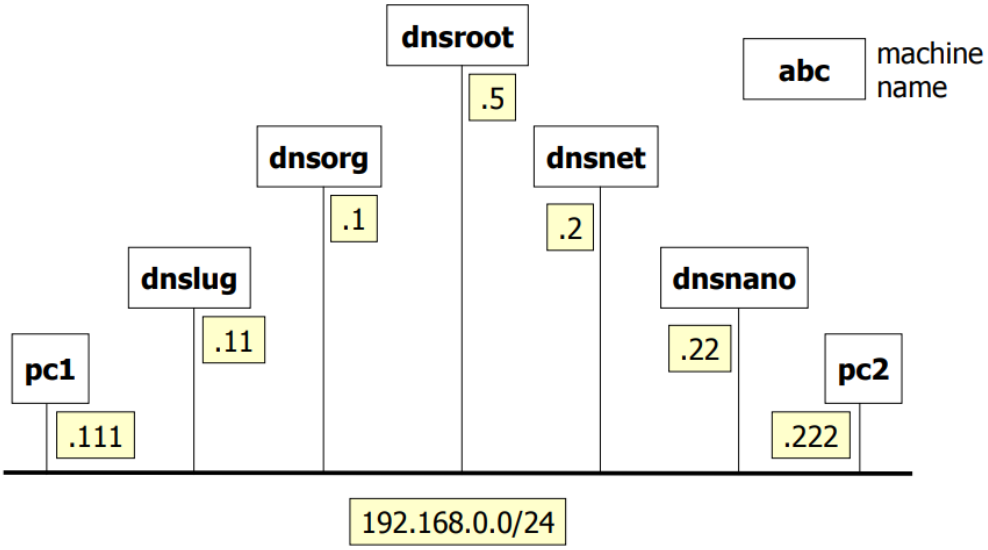
Domaines dans notre topologie

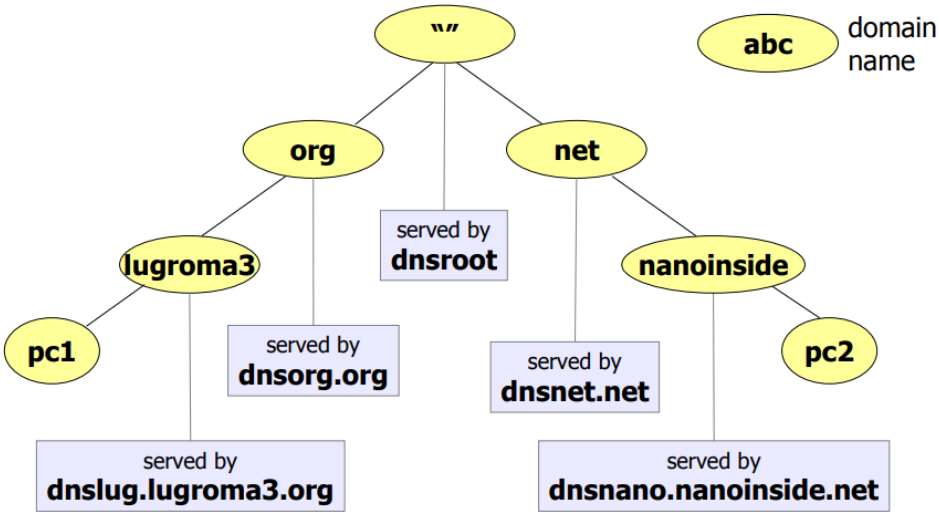


Zones dans notre topologie



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 ?

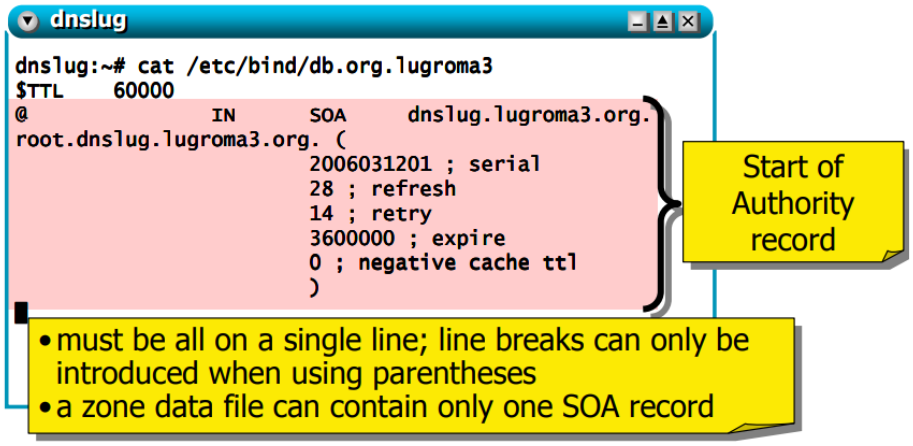
Explorer maintenant la configuration des *name servers*, en particulier en *dnslug* à l'aide de la commande suivante **:** cat /etc/bind/named.conf

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

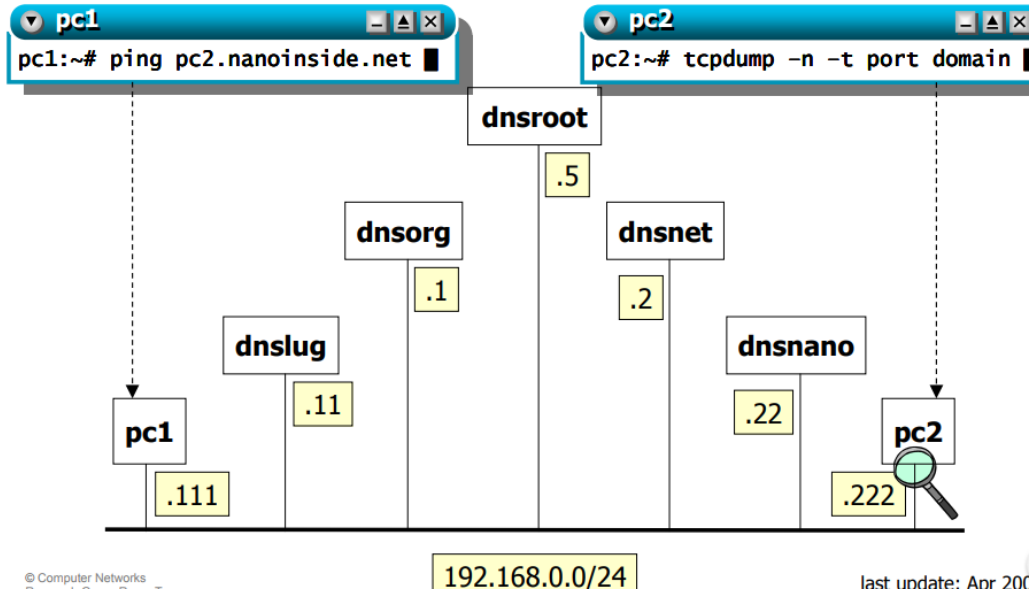
Qui est le *primary master* de la zone lugroma3.org ?

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

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

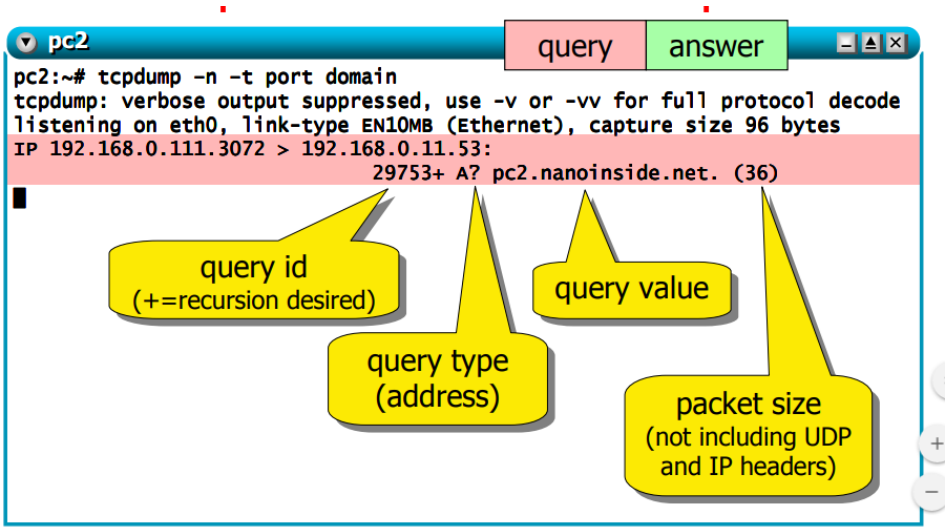


Step3 - Expérimentation

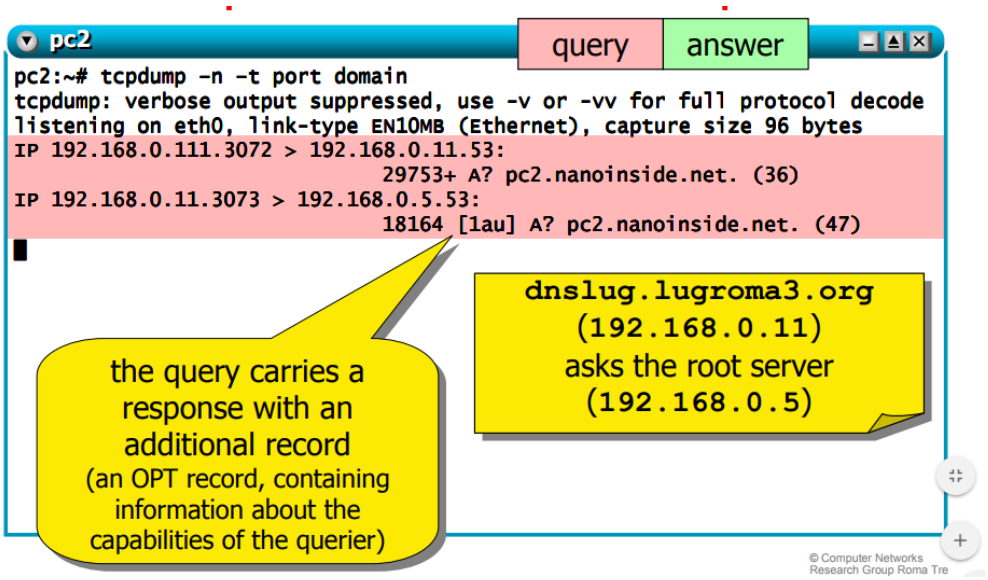


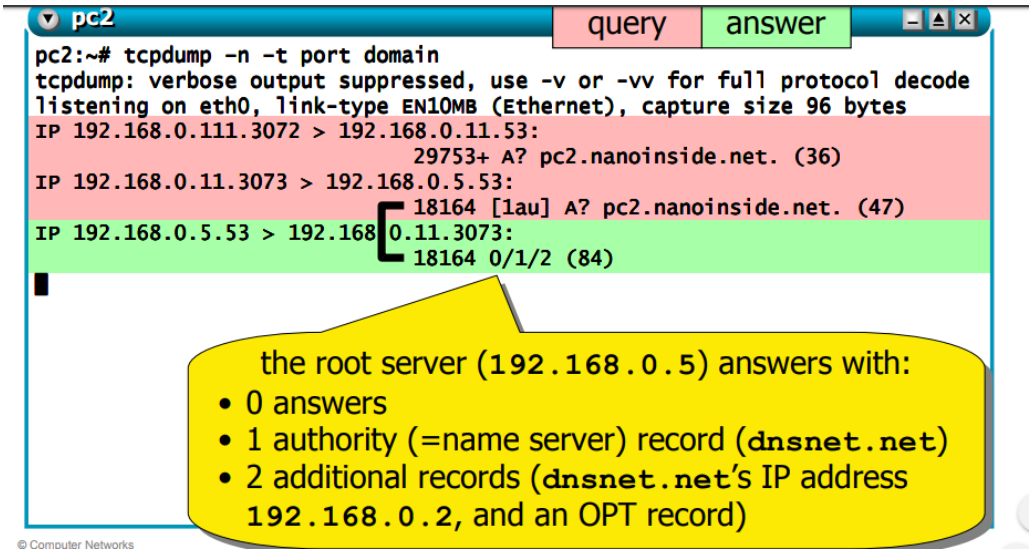
Tout d'abord on active la commande tcpdump –n –t port domain dans **pc2**

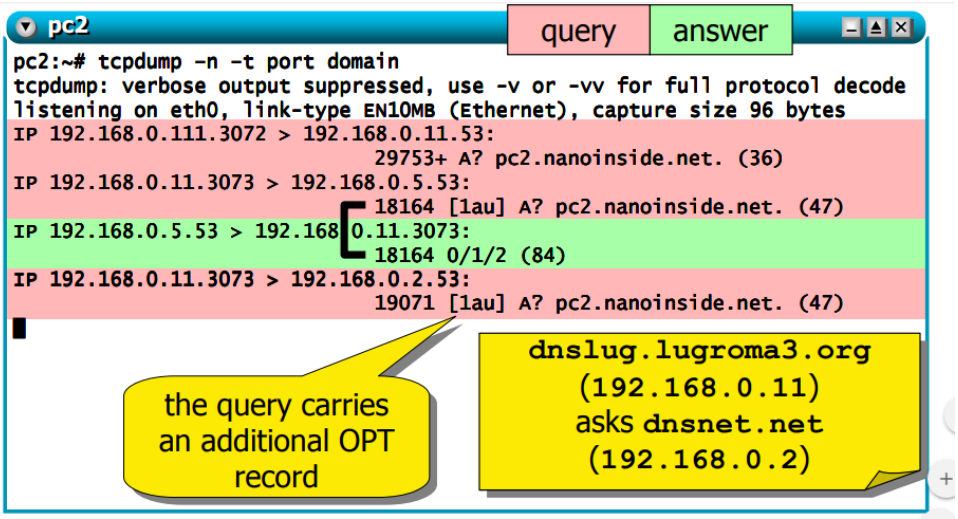
Ensuite on fait partir le ping dans **pc1** ping pc2.nanoinside.net

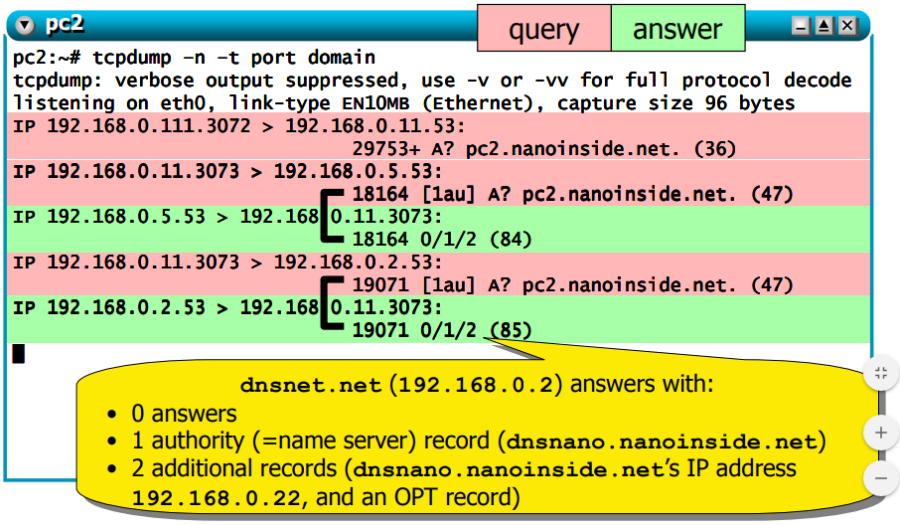


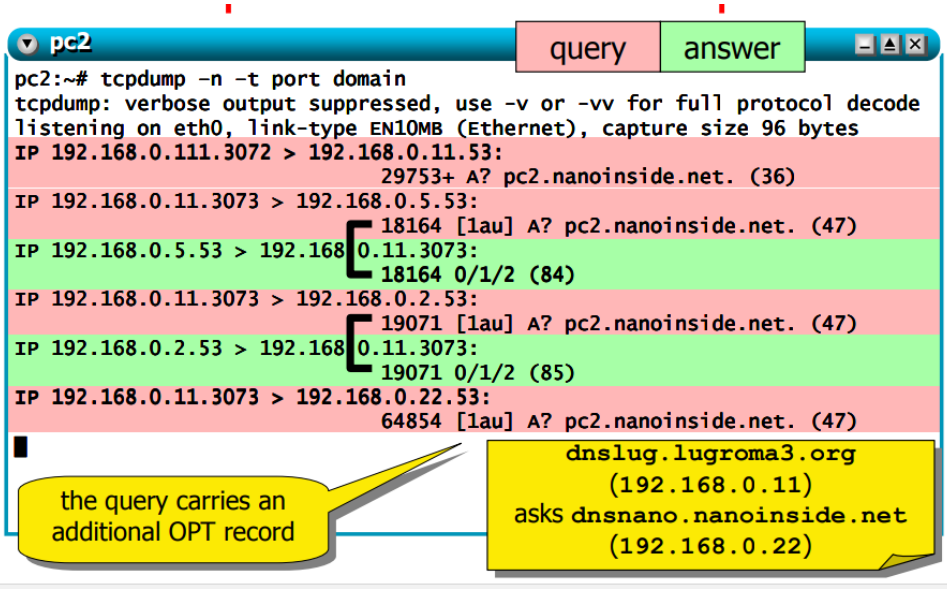
Les résultats de la capture sont les suivants :

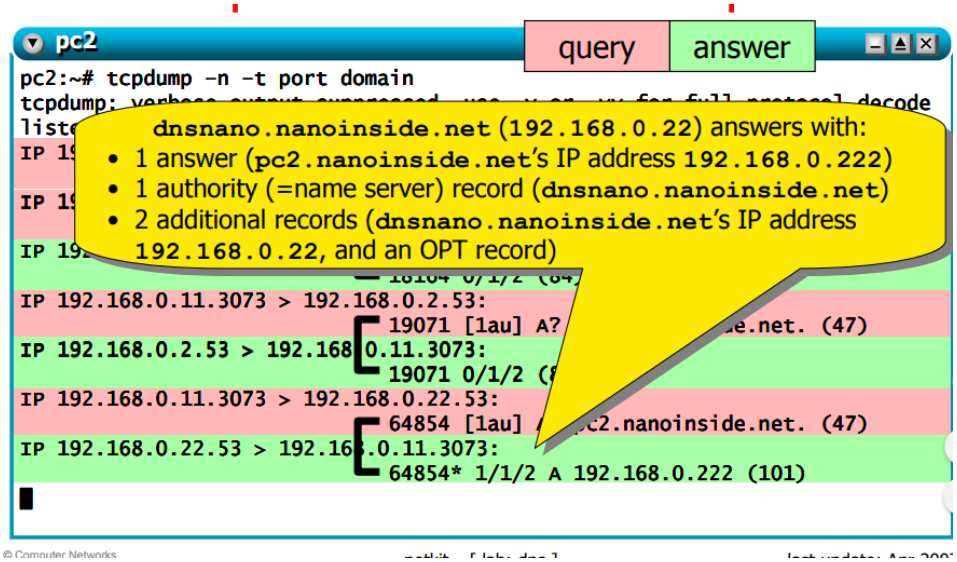


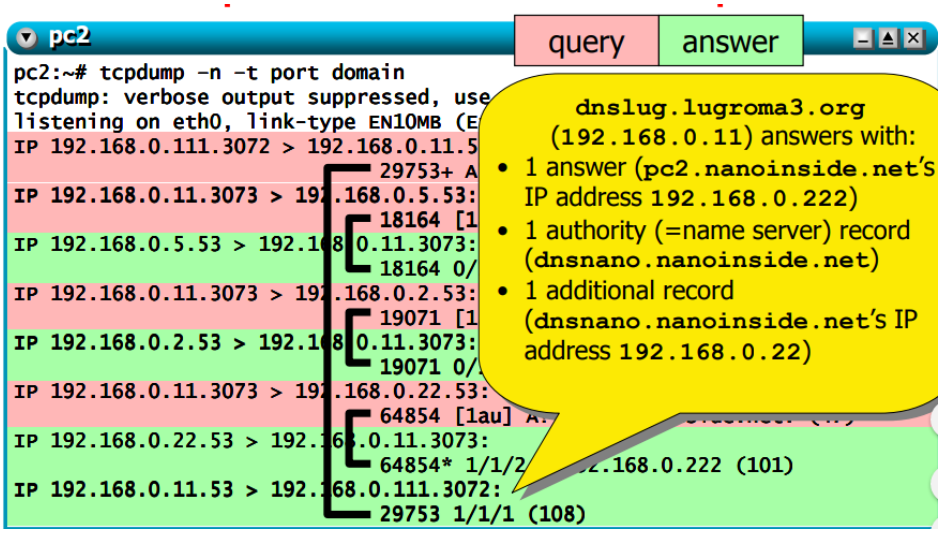




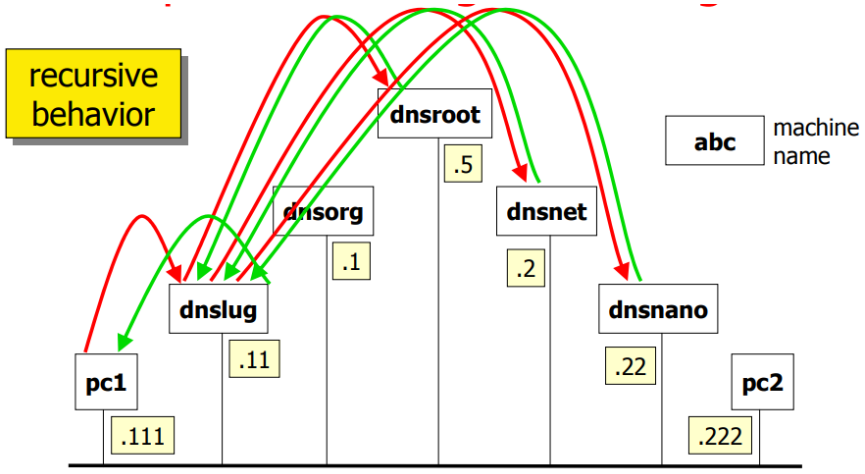



pc2
query
answer
pc2:~# tcpdump -n -t port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.111.3072 > 192.168.0.11.53:
29753+ A? pc2.nanoinside.net. (36)
IP 192.168.0.11.3073 > 192.168.0.5.53: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

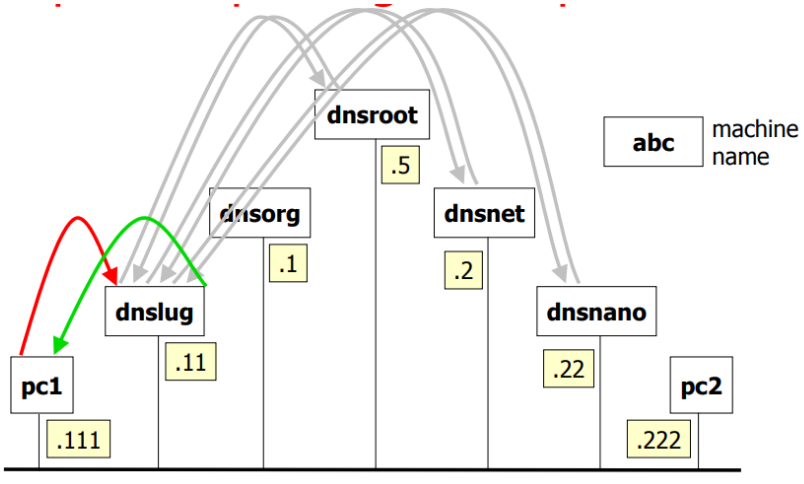


Le comportement est <u>récursif</u> : voici les messages échangés



Step 4 – Expérimentation

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



Sep 5 – redemarrer le name server

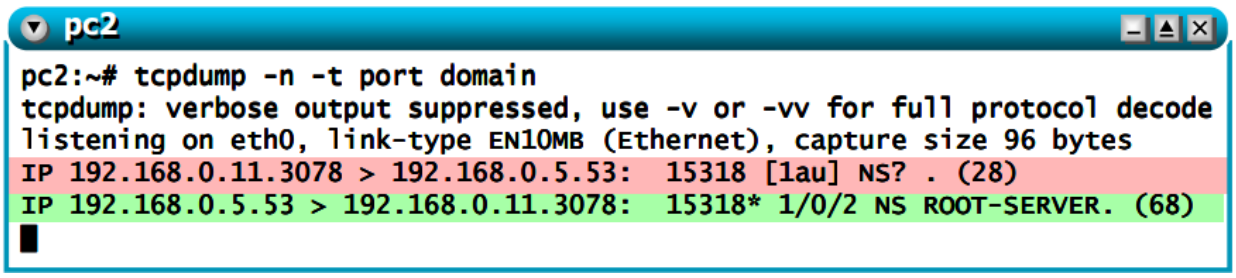
Le redemarrage permet de vider les caches. Une nouvelle query entrainera donc toutes les queries récursives comme vu précédemment.

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



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

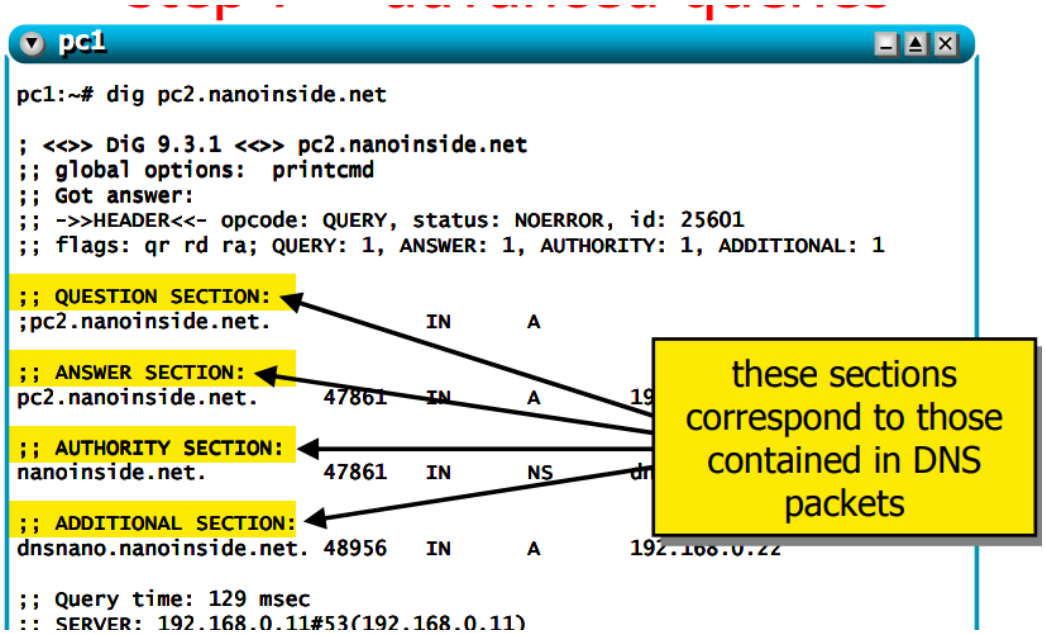
Q4 : ensuite, répétez la même expérimentation (ping vers *pluto.nanoinside.net*) et à l'aide de tcpdump en pc2 vérifiez les messages échangés (et le fait que le réponses soit maintenant déjà en cache).

Step 7 – Queries avancés

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

En pc1 *:* dig pc2.nanoinside.net

Observez le résultat :



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