

TP1 DNS

1) Configurez le serveur DNS primaire en vous appuyant sur l'annexe ou en consultant les liens indiqués.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA  dns1.rs.tp dns2.rs.tp (
                        2013251506      ; Serial
                        604800           ; Refresh
                        86400            ; Retry
                        2419200          ; Expire
                        604800 )         ; Negative Cache TTL
;
@      IN      NS   ns.rs.tp.
@      IN      NS   ns2.rs.tp.
ns     IN      A    192.168.63.140
ns2    IN      A    192.168.63.141
@      IN      A    192.168.63.140
dns1   IN      A    192.168.63.140
dns2   IN      A    192.168.63.141
```

2) Testez son fonctionnement en local (commandes : *nslookup* ou *dig* - utilisez man)

Exemple :

```
#nslookup primaire.tptr.fr
#nslookup secondaire.tptr.fr
```

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> rs.tp 2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6741
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
```

Beloeil Sebastien
Dorail Stéphane

;; QUESTION SECTION:

rs.tp. IN A

;; ANSWER SECTION:

rs.tp. 604800 IN A 192.168.63.140

;; AUTHORITY SECTION:

rs.tp. 604800 IN NS ns.rs.tp.

rs.tp. 604800 IN NS ns2.rs.tp.

;; ADDITIONAL SECTION:

ns.rs.tp. 604800 IN A 192.168.63.140

ns2.rs.tp. 604800 IN A 192.168.63.141

;; Query time: 0 msec

;; SERVER: 192.168.63.140#53(192.168.63.140)

;; WHEN: Mon Nov 25 15:36:20 2013

;; MSG SIZE rcvd: 106

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 25505

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

2. IN A

;; AUTHORITY SECTION:

. 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com.
2013112500 1800 900 604800 86400

;; Query time: 11 msec

;; SERVER: 192.168.63.140#53(192.168.63.140)

;; WHEN: Mon Nov 25 15:36:20 2013

;; MSG SIZE rcvd: 94

3) Configurez le client (utiliser l'annexe 2) et raccordez les deux postes au hub.

```
25/11/13 15:40:13 5830 # cat /etc/resolv.conf
nameserver 192.168.63.140
```

4) Interrogez le serveur primaire à partir du client et testez son fonctionnement.

```
25/11/13 15:37:16 5830 # ping dns1.rs.tp
PING dns1.rs.tp (192.168.63.140) 56(84) bytes of data.
64 bytes from 192.168.63.140: icmp_req=1 ttl=64 time=0.345 ms
^C
--- dns1.rs.tp ping statistics ---
```

Beloeil Sebastien
Dorail Stéphane

1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.345/0.345/0.345/0.000 ms

- 5) La machine qui servira de serveur DNS secondaire n'est pas connectée au hub :
- Configurez cette machine en tant que serveur secondaire (Annexe 4).
 - Exécutez la commande *ifconfig eth0 down*. Quelle est l'utilité de cette commande ?
 - Sur le client, lancez tcpdump (pour capturer les trames qui seront échangées lors du redémarrage du serveur DNS secondaire).
 - Connectez le serveur secondaire au réseau, réactivez l'interface (ifconfig eth0 up) et lancez le service de nom sur le serveur DNS secondaire

la commande ifconfig eth0 down, permet de désactiver l'interface réseaux de la machine et donc de la couper du réseau

Voir fichier **question5.dump**.

- 6) Vous sauvegarderez les trames échangées et proposerez un diagramme temporel .

- 7) Modifiez le fichier resolv.conf du client pour que :
- le premier serveur de nom interrogé soit le serveur secondaire ;
 - le deuxième le serveur de nom primaire.

```
25/11/13 15:55:04 5830 # cat /etc/resolv.conf
```

```
nameserver 192.168.63.141
```

```
nameserver 192.168.63.140
```

- 8) Le serveur primaire étant désactivé, lancez une interrogation à partir du client. Les trames échangées devront être sauvegardées et représentées sur un diagramme temporel.

Voir **question8**

- 9) Réactivez le serveur primaire, désactivez le secondaire. Formulez une nouvelle interrogation. Sauvegardez les trames échangées.

```
25/11/13 16:15:31 5830 # tcpdump -i vmnet8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmnet8, link-type EN10MB (Ethernet), capture size 65535 bytes
16:15:52.200525 ARP, Request who-has 192.168.63.141 tell 192.168.63.1, length 28
16:15:53.198967 ARP, Request who-has 192.168.63.141 tell 192.168.63.1, length 28
16:15:53.200751 ARP, Request who-has 192.168.63.140 tell 192.168.63.1, length 28
```

Beloeil Sebastien
Dorail Stéphane

```
16:15:53.201207 ARP, Reply 192.168.63.140 is-at 00:0c:29:ac:62:3e (oui Unknown), length 28
16:15:53.201228 IP 192.168.63.1.58584 > 192.168.63.140.domain: 7736+ A? dns2.rs.tp. (28)
16:15:53.202324 IP 192.168.63.140.domain > 192.168.63.1.58584: 7736* 1/2/2 A 192.168.63.141
(111)
16:15:54.198966 ARP, Request who-has 192.168.63.141 tell 192.168.63.1, length 28
16:15:57.202576 IP 192.168.63.1.51331 > 192.168.63.140.domain: 19911+ PTR?
141.63.168.192.in-addr.arpa. (45)
16:15:57.204293 IP 192.168.63.140.33012 > blackhole-2.iana.org.domain: 2500% [1au] PTR?
141.63.168.192.in-addr.arpa. (56)
16:15:57.215739 ARP, Request who-has 192.168.63.140 tell 192.168.63.2, length 28
16:15:57.216243 ARP, Reply 192.168.63.140 is-at 00:0c:29:ac:62:3e (oui Unknown), length 28
16:15:57.216322 IP blackhole-2.iana.org.domain > 192.168.63.140.33012: 2500 NXDomain*- 0/1/1
(133)
16:15:57.220235 IP 192.168.63.140.domain > 192.168.63.1.51331: 19911 NXDomain 0/1/0 (122)
```

10) Analysez les trames capturées dans la question 9).

le resolveur de dns ne peut pas trouver le premier serveur dns, a la 2ème non response du DNS, il décide d'interroger le serveur secondaire.

le serveur renvoie la réponse

11) Sur quels protocoles s'appuie le DNS ? Définissez brièvement le rôle de ces protocoles ?

le protocole s'appuie sur udp, parfois tcp dans le cas où il y a plein de loss.

12) Quel est le port utilisé par le service DNS ?

le port 53

13) Proposez quelques interrogations à l'aide de la commande nslookup ou dig.

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> dns1.rs.tp
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 37832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
dns1.rs.tp.                IN      A

;; ANSWER SECTION:
dns1.rs.tp.                604800 IN      A      192.168.63.140
```

Beloeil Sebastien
Dorail Stéphane

:: AUTHORITY SECTION:

rs.tp.	604800 IN	NS	ns2.rs.tp.
rs.tp.	604800 IN	NS	ns.rs.tp.

:: ADDITIONAL SECTION:

ns.rs.tp.	604800 IN	A	192.168.63.140
ns2.rs.tp.	604800 IN	A	192.168.63.141

:: Query time: 1 msec

:: SERVER: 192.168.63.141#53(192.168.63.141)

:: WHEN: Mon Nov 25 16:20:42 2013

:: MSG SIZE rcvd: 111

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> google.fr

:: global options: +cmd

:: Got answer:

:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40460

:: flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 4

:: QUESTION SECTION:

;google.fr.	IN	A
-------------	----	---

:: ANSWER SECTION:

google.fr.	300	IN	A	173.194.41.127
google.fr.	300	IN	A	173.194.41.119
google.fr.	300	IN	A	173.194.41.120

:: AUTHORITY SECTION:

google.fr.	172799 IN	NS	ns4.google.com.
google.fr.	172799 IN	NS	ns3.google.com.
google.fr.	172799 IN	NS	ns2.google.com.
google.fr.	172799 IN	NS	ns1.google.com.

:: ADDITIONAL SECTION:

ns1.google.com.	172799 IN	A	216.239.32.10
ns2.google.com.	172799 IN	A	216.239.34.10
ns3.google.com.	172799 IN	A	216.239.36.10
ns4.google.com.	172799 IN	A	216.239.38.10

:: Query time: 1007 msec

:: SERVER: 192.168.63.141#53(192.168.63.141)

:: WHEN: Mon Nov 25 16:20:52 2013

:: MSG SIZE rcvd: 221