
Administration système en réseau : synthèse DNS

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions		
\$Revision: 750 \$	\$Date: 2005-11-15 18:19:33 +0100 (mar, 15 nov 2005) \$	\$Author: latu \$
Année universitaire 2004-2005		

Table des matières

1. Copyright et Licence	2
1.1. Meta-information	2
2. Architecture type de travaux pratiques	3
3. Installation du service DNS <i>cache-only</i>	3
4. Requêtes DNS sur les différents types de <i>Resource Records</i> (RRs)	5
4.1. Types de la classe Internet IN	6
4.2. Types de la classe CHAOS	8
5. Délégation de la zone <i>zone(i).lan.stri</i>	9
5.1. Configuration de la délégation de zone	9
5.2. Validation de la délégation de zone	9
6. Ouverture de la zone <i>zone(i).lan.stri</i>	10
7. Documents de référence	11

1. Copyright et Licence

Copyright (c) 2000,2005 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2005 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.1 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Meta-information

Cet article est écrit avec *DocBook*¹ XML sur un système *Debian GNU/Linux*². Il est disponible en version imprimable aux formats PDF et Postscript : [admin.reseau.synthese-dns.pdf](#)³ | [admin.reseau.synthese-dns.ps.gz](#)⁴.

¹ <http://www.docbook.org>

² <http://www.debian.org>

³ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.synthese-dns.pdf>

⁴ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.synthese-dns.ps.gz>

2. Architecture type de travaux pratiques

Comme indiqué dans le support sur l'*Administration système en réseau : architecture réseau*, on part d'une configuration avec deux de postes de travail qui partagent le même domaine de diffusion. Le schéma est le suivant :

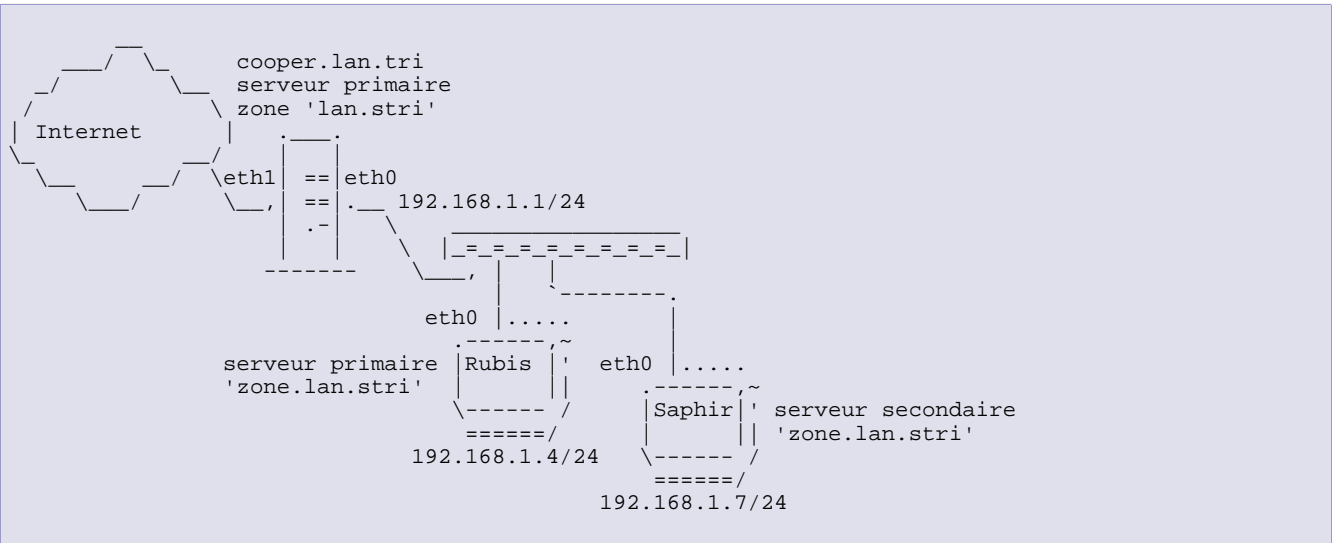


Tableau 1. Affectation des adresses

Rubis	Saphir	Passerelle par défaut
192.168.1.4/24	192.168.1.7/24	192.168.1.1/24

3. Installation du service DNS *cache-only*

On sait que le logiciel à utiliser est appelé *Berkeley Internet Name Domain* (BIND). On oriente donc la recherche dans la base de données des paquets Debian vers la chaîne de caractère `bind*`.

```
saphir:~$ dpkg -l bind*
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/écheC-conFig/H=semi-installé
| / Err?=(aucune)/H=à garder/besoin Réinstallation/X=les deux (État,Err: majuscule=mauvais)
||/ Nom                               Version                               Description
|+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
pn bind                                <néant>                                (aucune description n'est disponible)
pn bind-dev                             <néant>                                (aucune description n'est disponible)
pn bind-doc                              <néant>                                (aucune description n'est disponible)
pn bind9                                 <néant>                                (aucune description n'est disponible)
pn bind9-doc                             <néant>                                (aucune description n'est disponible)
ii bind9-host                            9.3.1-2                               Version of 'host' bundled with BIND 9.X
pn bindgraph                             <néant>                                (aucune description n'est disponible)
```

Les paquetages à installer à partir de la liste ci-dessus sont : `bind9` et `bind9-doc`. Une fois l'opération `# apt-get install bind9 bind9-doc` effectuée, on vérifie le résultat.

```
saphir:~# dpkg -l bind* |grep ^ii
ii bind9                                9.3.1-2                               Internet Domain Name Server
ii bind9-doc                             9.3.1-2                               Documentation for BIND
ii bind9-host                            9.3.1-2                               Version of 'host' bundled with BIND 9.X
```

On valide l'activité du service à partir de la liste des processus, des ports ouverts en écoute sur le réseau et des messages système. La «singularité» du service DNS provient du nom du processus exécuté : `named`.

Liste des processus actifs

```
saphir:~# ps aux |grep named
bind 7503 0.0 0.6 29816 2812 ? Ssl 09:46 0:00 /usr/sbin/named -u bind
```

Ports réseau ouverts en écoute

```
saphir:~# lsof -i |grep named
named 7503 bind 20u IPv4 13663 UDP localhost.localdomain:domain
named 7503 bind 21u IPv4 13664 TCP localhost.localdomain:domain (LISTEN)
named 7503 bind 22u IPv4 13665 UDP 192.168.1.7:domain
named 7503 bind 23u IPv4 13666 TCP 192.168.1.7:domain (LISTEN)
named 7503 bind 24u IPv4 13667 UDP *:1072
named 7503 bind 25u IPv6 13668 UDP *:1073
named 7503 bind 26u IPv4 13669 TCP localhost.localdomain:953 (LISTEN)
named 7503 bind 27u IPv6 13670 TCP ip6-localhost:953 (LISTEN)
```

```
saphir:~# netstat -autp |grep named
tcp 0 0 192.168.1.7:domain *:* LISTEN 7503/named
tcp 0 0 localhost.localdomain *:* LISTEN 7503/named
tcp 0 0 localhost.localdomain:953 *:* LISTEN 7503/named
tcp6 0 0 ip6-localhost:953 *:* LISTEN 7503/named
udp 0 0 *:1072 *:* 7503/named
udp 0 0 192.168.1.7:domain *:* 7503/named
udp 0 0 localhost.localdomain *:* 7503/named
udp6 0 0 *:1073 *:* 7503/named
```

Messages systèmes

```
saphir:~# tail -150 /var/log/daemon.log |grep named
May 26 09:46:59 localhost named[7503]: starting BIND 9.3.1 -u bind
May 26 09:46:59 localhost named[7503]: found 1 CPU, using 1 worker thread
May 26 09:46:59 localhost named[7503]: loading configuration from '/etc/bind/named.conf'
May 26 09:46:59 localhost named[7503]: listening on IPv4 interface lo, 127.0.0.1#53
May 26 09:46:59 localhost named[7503]: listening on IPv4 interface wlan0, 192.168.1.7#53
May 26 09:46:59 localhost named[7503]: command channel listening on 127.0.0.1#953
May 26 09:46:59 localhost named[7503]: command channel listening on ::1#953
May 26 09:46:59 localhost named[7503]: zone 0.in-addr.arpa/IN: loaded serial 1
May 26 09:46:59 localhost named[7503]: zone 127.in-addr.arpa/IN: loaded serial 1
May 26 09:46:59 localhost named[7503]: zone 255.in-addr.arpa/IN: loaded serial 1
May 26 09:46:59 localhost named[7503]: zone localhost/IN: loaded serial 1
May 26 09:46:59 localhost named[7503]: running
```

Comme tout service implanté sur un système GNU/Linux, les fichiers de configuration sont placés dans le répertoire `/etc/`.

```
saphir:~# dpkg -L bind9 |grep etc
/etc
/etc/bind
/etc/bind/db.0
/etc/bind/db.255
/etc/bind/db.empty
/etc/bind/zones.rfc1918
/etc/bind/db.127
/etc/bind/db.local
/etc/bind/db.root
/etc/bind/named.conf
/etc/bind/named.conf.local
/etc/bind/named.conf.options
/etc/init.d
/etc/init.d/bind9
```

De la même façon, les données du services doivent être placées dans le répertoire `/var/`.

```
saphir:~# dpkg -L bind9 |grep var
/var
/var/cache
/var/cache/bind❶
/var/run
/var/run/bind
/var/run/bind/run❷
```

- ❶ C'est dans le répertoire `/var/cache/bind/` que l'on place les fichiers de déclaration des zones sur lesquelles le serveur a autorité. Voir option `directory` dans le fichier `/etc/bind/named.conf.options`.
- ❷ C'est dans le fichier `/var/run/bind/run/named.pid` que l'on retrouve le numéro de processus du service. Cette information est placée là par le script d'initialisation du service (cf. *runlevels*).

```
saphir:~# cat /var/run/bind/run/named.pid
7503
```

Le service DNS, tel qu'il est installé par défaut, est de type *cache-only* :

- Il ne contient aucune déclaration de zone. Le répertoire `/var/cache/bind/` est vide.
- La liste des fichiers de configuration indique que le service possède la liste des serveurs racine via le fichier `db.root`.
- Le processus étant actif, il va pouvoir prendre en charge les requêtes et mémoriser dans son cache les résultats. Du côté «local», on optimise le traitement des requêtes en ayant recours à ce cache. Du côté «Internet», on surcharge les serveurs racines en les sollicitant directement à chaque nouvelle requête.

C'est le fichier `/etc/resolv.conf` qui configure le *resolver*. En partant de la configuration initiale du poste (voir [Section 2, « Architecture type de travaux pratiques »](#)), le *resolver* fait référence au service DNS du serveur `192.168.1.1` :

```
saphir:~# cat /etc/resolv.conf
search lan.stri
nameserver 192.168.1.1
```

On édite ce même fichier pour qu'il fasse référence au service local :

```
saphir:~# cat /etc/resolv.conf
search lan.stri
nameserver 127.0.0.1
```

La commande **dig** est le «couteau suisse» qui va permettre d'effectuer tous les tests de requêtes DNS. On obtient le nom du paquet auquel elle appartient à partir d'une recherche du type :

```
saphir:~# dpkg -S `which dig`
dnsutils: /usr/bin/dig
```

Le paquet `dnsutils` fait partie de l'installation de base. Il est donc présent sur tous les systèmes.

4. Requêtes DNS sur les différents types de *Resource Records* (RRs)

L'utilisation du cache du serveur DNS est identifiable à partir du temps de traitement d'une requête. Ce temps de traitement apparaît dans le champ `Query time` des résultats affichés à la suite d'un appel à la commande **dig**.

Dans les deux exemples ci-dessous, le serveur interrogé est bien le service local avec l'adresse IP `127.0.0.1`. La première requête a un temps de traitement de 2329ms tandis que la seconde a un temps de traitement de 4ms. Cette seconde réponse est fournie par le cache du serveur DNS.

```
saphir:~# dig www.linux-france.org

<snipped/>
;; Query time: 2329 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 26 14:16:15 2005
;; MSG SIZE rcvd: 146
```

```
saphir:~# dig www.linux-france.org

<snipped/>
;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 26 14:17:12 2005
;; MSG SIZE rcvd: 146
```

Les différents enregistrements ou *Resource Records* d'une zone sont accessibles à partir de requêtes individuelles. Les options de la commande **dig**, documentées dans les pages de manuels (`man dig`), permettent d'indiquer le type d'enregistrement demandé (RR) après le nom de domaine. Les réponses aux requêtes suivantes apparaissent après la mention `ANSWER SECTION:`.

4.1. Types de la classe Internet IN

Requête sur un serveur de noms, NS

```
saphir:~$ dig nic.fr ns

; <<>> DiG 9.3.1 <<>> nic.fr ns
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23117
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nic.fr.                                IN      NS

;; ANSWER SECTION:
nic.fr.      91677  IN      NS      dns.inria.fr.
nic.fr.      91677  IN      NS      ns0.oleane.net.
nic.fr.      91677  IN      NS      ns1.nic.fr.
nic.fr.      91677  IN      NS      ns1.oleane.net.
nic.fr.      91677  IN      NS      ns2.nic.fr.
nic.fr.      91677  IN      NS      ns3.nic.fr.
nic.fr.      91677  IN      NS      ns-sec.ripe.net.

;; Query time: 137 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat May 28 16:15:05 2005
;; MSG SIZE rcvd: 174
```

Requête sur un nom d'hôte, A

```
saphir:~$ dig www.nic.fr

; <<>> DiG 9.3.1 <<>> www.nic.fr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61145
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 10

;; QUESTION SECTION:
;www.nic.fr.                            IN      A

;; ANSWER SECTION:
www.nic.fr.      172791 IN      CNAME   rigolo.nic.fr.
rigolo.nic.fr.   172101 IN      A       192.134.4.20

;; AUTHORITY SECTION:
nic.fr.          91532  IN      NS      ns0.oleane.net.
nic.fr.          91532  IN      NS      ns1.nic.fr.
nic.fr.          91532  IN      NS      ns1.oleane.net.
nic.fr.          91532  IN      NS      ns2.nic.fr.
nic.fr.          91532  IN      NS      ns3.nic.fr.
nic.fr.          91532  IN      NS      ns-sec.ripe.net.
nic.fr.          91532  IN      NS      dns.inria.fr.

;; ADDITIONAL SECTION:
dns.inria.fr.    172791 IN      A       193.51.208.13
ns0.oleane.net. 349     IN      A       194.2.0.30
ns1.nic.fr.     345592 IN      A       192.93.0.1
ns1.oleane.net. 592     IN      A       194.2.0.60
ns2.nic.fr.     345592 IN      A       192.93.0.4
ns2.nic.fr.     345592 IN      AAAAA  2001:660:3005:1::1:2
ns3.nic.fr.     345592 IN      A       192.134.0.49
ns3.nic.fr.     345592 IN      AAAAA  2001:660:3006:1::1:1
ns-sec.ripe.net. 125568 IN      A       193.0.0.196
ns-sec.ripe.net. 130131 IN      AAAAA  2001:610:240:0:53::4

;; Query time: 14 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat May 28 16:17:30 2005
;; MSG SIZE rcvd: 411
```

Requête sur une adresse IP, PTR

```
saphir:~$ dig -x 192.134.4.20

; <<>> DiG 9.3.1 <<>> -x 192.134.4.20
;; global options: printcmd
;; Got answer:
```

```
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 14789
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;20.4.134.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
20.4.134.192.in-addr.arpa. 172800 IN      PTR      rigolo.nic.fr.

;; Query time: 169 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat May 28 16:51:10 2005
;; MSG SIZE rcvd: 70
```

Requête sur un agent de transfert de courrier électronique, MX

```
saphir:~$ dig nic.fr MX

; <<>> DiG 9.3.1 <<>> nic.fr MX
;; global options: printcmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 59667
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 8

;; QUESTION SECTION:
;nic.fr.                        IN      MX

;; ANSWER SECTION:
nic.fr.          120655 IN      MX      50 mx1.nic.fr.
nic.fr.          120655 IN      MX      100 mx2.nic.fr.

;; AUTHORITY SECTION:
nic.fr.          89308  IN      NS      ns1.oleane.net.
nic.fr.          89308  IN      NS      ns2.nic.fr.
nic.fr.          89308  IN      NS      ns3.nic.fr.
nic.fr.          89308  IN      NS      ns-sec.ripe.net.
nic.fr.          89308  IN      NS      dns.inria.fr.
nic.fr.          89308  IN      NS      ns0.oleane.net.
nic.fr.          89308  IN      NS      ns1.nic.fr.

;; ADDITIONAL SECTION:
dns.inria.fr.    170567 IN      A       193.51.208.13
ns1.nic.fr.     343368 IN      A       192.93.0.1
ns2.nic.fr.     343368 IN      A       192.93.0.4
ns2.nic.fr.     343368 IN      AAAA    2001:660:3005:1::1:2
ns3.nic.fr.     343368 IN      A       192.134.0.49
ns3.nic.fr.     343368 IN      AAAA    2001:660:3006:1::1:1
ns-sec.ripe.net. 123344 IN      A       193.0.0.196
ns-sec.ripe.net. 127907 IN      AAAA    2001:610:240:0:53::4

;; Query time: 73 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat May 28 16:54:34 2005
;; MSG SIZE rcvd: 378
```

Pour émettre une requête itérative (ou non récursive), il faut utiliser l'option `+trace`.

```
# dig +trace www.nic.fr

; <<>> DiG 9.3.1 <<>> +trace www.nic.fr
;; global options: printcmd
.          518400 IN      NS      L.ROOT-SERVERS.NET.
.          518400 IN      NS      M.ROOT-SERVERS.NET.
.          518400 IN      NS      A.ROOT-SERVERS.NET.
.          518400 IN      NS      B.ROOT-SERVERS.NET.
.          518400 IN      NS      C.ROOT-SERVERS.NET.
.          518400 IN      NS      D.ROOT-SERVERS.NET.
.          518400 IN      NS      E.ROOT-SERVERS.NET.
.          518400 IN      NS      F.ROOT-SERVERS.NET.
.          518400 IN      NS      G.ROOT-SERVERS.NET.
.          518400 IN      NS      H.ROOT-SERVERS.NET.
.          518400 IN      NS      I.ROOT-SERVERS.NET.
.          518400 IN      NS      J.ROOT-SERVERS.NET.
.          518400 IN      NS      K.ROOT-SERVERS.NET.
;; Received 228 bytes from 127.0.0.1#53(127.0.0.1) in 94 ms

fr.        172800 IN      NS      A.EXT.nic.fr.
fr.        172800 IN      NS      C.EXT.nic.fr.
fr.        172800 IN      NS      C.nic.fr.
fr.        172800 IN      NS      A.nic.fr.
fr.        172800 IN      NS      B.nic.fr.
fr.        172800 IN      NS      D.EXT.nic.fr.
fr.        172800 IN      NS      E.EXT.nic.fr.
```

```
;; Received 340 bytes from 198.32.64.12#53(L.ROOT-SERVERS.NET) in 246 ms
www.nic.fr.          172800 IN      CNAME   rigolo.nic.fr.
rigolo.nic.fr.      172800 IN      A       192.134.4.20
nic.fr.             172800 IN      NS      ns0.oleane.net.
nic.fr.             172800 IN      NS      ns1.nic.fr.
nic.fr.             172800 IN      NS      ns1.oleane.net.
nic.fr.             172800 IN      NS      ns2.nic.fr.
nic.fr.             172800 IN      NS      ns3.nic.fr.
nic.fr.             172800 IN      NS      ns-sec.ripe.net.
nic.fr.             172800 IN      NS      dns.inria.fr.
;; Received 367 bytes from 193.51.208.13#53(A.EXT.nic.fr) in 80 ms
```

Après tous ces exemples de requêtes, on voit clairement que le fonctionnement par défaut du logiciel BIND est récursif. Cette prise en charge «ouverte» des requêtes peut poser quelques soucis de sécurité. Si il est légitime de prendre complètement en charge les interrogations DNS émises par les hôtes du réseau administré de façon à nourrir le cache et optimiser le fonctionnement du service, il n'en va pas de même pour les hôtes du réseau public. Il est donc important de configurer le service en conséquence. [FIXME: xref vers config]

4.2. Types de la classe CHAOS

Toutes les exemples de requêtes donnés ci-avant utilisent la classe Internet (IN) de façon implicite. Pour interroger un type de la classe CHAOS, il est nécessaire d'indiquer cette classe dans la commande d'interrogation du service DNS. Voici deux exemples de requêtes sur les deux types les plus recherchés.

```
saphir:~# dig @localhost. version.bind txt chaos +novc
; <<>> DiG 9.3.1 <<>> @localhost. version.bind txt chaos +novc
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 60929
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.          CH      TXT

;; ANSWER SECTION:
version.bind.          0      CH      TXT      "9.3.1"

;; AUTHORITY SECTION:
version.bind.          0      CH      NS      version.bind.

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jun  2 14:45:47 2005
;; MSG SIZE rcvd: 62
```

```
saphir:~# dig @localhost. authors.bind txt chaos +novc
; <<>> DiG 9.3.1 <<>> @localhost. authors.bind txt chaos +novc
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 17999
;; flags: qr aa rd; QUERY: 1, ANSWER: 12, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;authors.bind.         CH      TXT

;; ANSWER SECTION:
authors.bind.          0      CH      TXT      "Damien Neil"
authors.bind.          0      CH      TXT      "Matt Nelson"
authors.bind.          0      CH      TXT      "Michael Sawyer"
authors.bind.          0      CH      TXT      "Brian Wellington"
authors.bind.          0      CH      TXT      "Mark Andrews"
authors.bind.          0      CH      TXT      "James Brister"
authors.bind.          0      CH      TXT      "Ben Cottrell"
authors.bind.          0      CH      TXT      "Michael Graff"
authors.bind.          0      CH      TXT      "Andreas Gustafsson"
authors.bind.          0      CH      TXT      "Bob Halley"
authors.bind.          0      CH      TXT      "David Lawrence"
authors.bind.          0      CH      TXT      "Danny Mayer"

;; AUTHORITY SECTION:
authors.bind.          0      CH      NS      authors.bind.

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
```

```
;; WHEN: Thu Jun 2 14:46:49 2005
;; MSG SIZE rcvd: 355
```

Les valeurs associées à ces types peuvent donner des renseignements précieux pour une éventuelle attaque sur le service DNS. Il est donc vivement conseillé de masquer ces valeurs lorsque l'on exploite un service DNS directement accessible depuis l'Internet. [FIXME: xref vers config].

5. Délégation de la zone `zone(i).lan.stri`



Avertissement

Cette partie est complétée par l'enseignant sur le serveur DNS principal de travaux pratiques.

Le serveur maître de la zone `lan.stri` doit déléguer le domaine `zone(i).lan.stri` au poste de travaux pratique qui doit devenir maître de ce sous domaine.

5.1. Configuration de la délégation de zone

Fichier `/etc/bind/named.conf.local` :

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "192.168.1";
};

zone "lan.stri" {
    type master;
    file "lan.stri";
};

zone "zone.lan.stri" {
    type slave;
    file "zone.lan.stri.backup";
    masters { 192.168.1.4; };
};
```

Un simple redémarrage du service permet de prendre en compte cette nouvelle zone déléguée.

```
cooper:/etc/bind# /etc/init.d/bind9 restart
```

Le journal système `syslog` ne doit pas faire apparaître d'erreur.

```
cooper:/etc/bind# tail -150 /var/log/syslog |grep named
Jun 2 16:29:15 cooper named[20525]: starting BIND 9.3.1 -u bind
Jun 2 16:29:15 cooper named[20525]: found 1 CPU, using 1 worker thread
Jun 2 16:29:15 cooper named[20525]: loading configuration from '/etc/bind/named.conf'
Jun 2 16:29:15 cooper named[20525]: listening on IPv4 interface lo, 127.0.0.1#53
Jun 2 16:29:15 cooper named[20525]: listening on IPv4 interface eth0, 192.168.1.1#53
Jun 2 16:29:15 cooper named[20525]: command channel listening on 127.0.0.1#953
Jun 2 16:29:15 cooper named[20525]: command channel listening on ::1#953
```

5.2. Validation de la délégation de zone

Lorsque la nouvelle zone `zone(i).lan.stri` est ouverte, on peut «provoquer» les opérations de transfert en redémarrant le service. Le journal système du serveur qui a autorité sur la zone déléguée doit faire apparaître un message de début et de fin de transfert.

```
Jun 2 17:28:41 rubis named[12060]: client 192.168.1.1#4209: transfer of 'zone.lan.stri/IN': AXFR started
Jun 2 17:28:41 rubis named[12060]: client 192.168.1.1#4209: transfer of 'zone.lan.stri/IN': AXFR ended
```

Le serveur qui a délégué la zone devient serveur secondaire de la zone et possède une copie des *Resource Records* du serveur primaire. Cette copie est le résultat de l'opération de transfert journalisée ci-avant.

```
cooper:/etc/bind# cat /var/cache/bind/zone.lan.stri.backup
$ORIGIN .
$TTL 86400      ; 1 day
zone.lan.stri  IN SOA  zone.lan.stri. root.zone.lan.stri. (
```

```

                2005060201 ; serial
                28800      ; refresh (8 hours)
                7200       ; retry (2 hours)
                604800     ; expire (1 week)
                86400     ; minimum (1 day)
                )
NS              zone.lan.stri.
A              192.168.1.4
MX             10 smtp.zone.lan.stri.
TXT           "zone.lan.stri Lab"
$ORIGIN zone.lan.stri.
ns            CNAME zone.lan.stri.
smtp        CNAME zone.lan.stri.

```

On peut aussi consulter cette copie à l'aide de requêtes locales :

```

cooper:/etc/bind# dig zone.lan.stri. ns

; <<>> DiG 9.3.1 <<>> zone.lan.stri. ns
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61701
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;zone.lan.stri.                IN      NS

;; ANSWER SECTION:
zone.lan.stri.                86400   IN      NS      zone.lan.stri.

;; ADDITIONAL SECTION:
zone.lan.stri.                86400   IN      A       192.168.1.4

;; Query time: 8 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jun  2 17:59:53 2005
;; MSG SIZE rcvd: 61

```

6. Ouverture de la zone zone(i).lan.stri

Le fichier `/etc/bind/named.conf.local` du nouveau serveur DNS doit être édité pour déclarer qu'il a autorité sur la zone `zone.lan.stri` :

```

zone "zone.lan.stri" {
    type master;
    file "zone.lan.stri";
};

```

En respectant les options de configuration du paquet Debian, on crée le fichier `/var/cache/bind/zone.lan.stri`.

```

$TTL 1D
@      IN      SOA      zone.lan.stri. root.zone.lan.stri. (
                2005060201      ; serial, yearmonthdayserial#
                8H              ; refresh, seconds
                2H              ; retry, seconds
                1W              ; expire, seconds
                1D )            ; minimum, seconds
NS     zone.lan.stri.
MX     10 smtp.zone.lan.stri. ; Primary Mail Exchanger
TXT    "zone.lan.stri Lab"

zone.lan.stri.      A      192.168.1.4
rubis              CNAME  zone.lan.stri.
ns                 CNAME  zone.lan.stri.
smtp               CNAME  zone.lan.stri.

saphir             A      192.168.1.7

```

On peut alors redémarrer le service et vérifier qu'il n'y a pas de message d'erreur dans les journaux :

```

rubis:/var/cache/bind# /etc/init.d/bind9 restart
rubis:/var/cache/bind# tail -150 /var/log/syslog |grep named
Jun  2 17:24:52 rubis named[4380]: shutting down: flushing changes
Jun  2 17:24:52 rubis named[4380]: stopping command channel on 127.0.0.1#953
Jun  2 17:24:52 rubis named[4380]: stopping command channel on ::1#953
Jun  2 17:24:52 rubis named[4380]: no longer listening on 127.0.0.1#53
Jun  2 17:24:52 rubis named[4380]: exiting

```

```

Jun  2 17:24:54 rubis named[12060]: starting BIND 9.3.1 -u bind
Jun  2 17:24:54 rubis named[12060]: found 1 CPU, using 1 worker thread
Jun  2 17:24:54 rubis named[12060]: loading configuration from '/etc/bind/named.conf'
Jun  2 17:24:54 rubis named[12060]: listening on IPv4 interface lo, 127.0.0.1#53
Jun  2 17:24:54 rubis named[12060]: listening on IPv4 interface eth0, 192.168.1.4#53
Jun  2 17:24:54 rubis named[12060]: command channel listening on 127.0.0.1#953
Jun  2 17:24:54 rubis named[12060]: command channel listening on :::1#953
Jun  2 17:24:54 rubis named[12060]: zone 0.in-addr.arpa/IN: loaded serial 1
Jun  2 17:24:54 rubis named[12060]: zone 127.in-addr.arpa/IN: loaded serial 1
Jun  2 17:24:54 rubis named[12060]: zone 255.in-addr.arpa/IN: loaded serial 1
Jun  2 17:24:54 rubis named[12060]: zone localhost/IN: loaded serial 1
Jun  2 17:24:54 rubis named[12060]: zone zone.lan.stri/IN: loaded serial 2005060201
Jun  2 17:24:54 rubis named[12060]: running

```

Ce n'est qu'après avoir vérifié que la zone est bien prise en charge avec le bon numéro de série que l'on peut effectuer les tests de requêtes.

```

rubis:/var/cache/bind# dig zone.lan.stri. ns

; <<>> DiG 9.3.1 <<>> zone.lan.stri. ns
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 4031
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;zone.lan.stri.                IN      NS

;; ANSWER SECTION:
zone.lan.stri.                86400   IN      NS      zone.lan.stri.

;; ADDITIONAL SECTION:
zone.lan.stri.                86400   IN      A       192.168.1.4

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jun  2 17:37:11 2005
;; MSG SIZE rcvd: 61

```

On valide les enregistrements ou *Resource Records* un à un en reprenant les syntaxes de requêtes présentées dans la Section 4, « Requêtes DNS sur les différents types de *Resource Records* (RRs) ».

7. Documents de référence

BIND 9 Administrator Reference Manual

*BIND 9 Administrator Reference Manual*⁵ : documentation complète la plus récente sur la syntaxe de configuration du service DNS. Si le paquet `bind9-doc` est installé, ce manuel est placé dans le répertoire `/usr/share/doc/bind9-doc/arm/`.

DNS HOWTO

*DNS HOWTO*⁶ : documentation complète sur la configuration serveur et client DNS.

Securing an Internet Name Server

*Securing an Internet Name Server*⁷ : documentation de référence sur la configuration des fonctions de sécurité d'un service DNS.

Secure BIND Template

*Secure BIND Template*⁸ : patrons de fichiers de configuration d'un service DNS.

Administration système en réseau : architecture réseau

*Administration système en réseau : architecture réseau*⁹ : présentation de l'architecture des travaux pratiques de la série.

Configuration d'une interface réseau

*Configuration d'une interface réseau*¹⁰ : tout sur la configuration des interfaces réseau ; notamment les

⁵ <http://www.bind9.net/manuals>

⁶ <http://www.tldp.org/HOWTO/DNS-HOWTO.html>

⁷ <http://www.cert.org/archive/pdf/dns.pdf>

⁸ <http://www.cymru.com/Documents/secure-bind-template.html>

⁹ <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.archi/>

explications sur les opérations «rituelles» de début de travaux pratiques :

```
# /etc/init.d/networking stop
# ifconfig lo up
# ifconfig eth0 192.168.0.2 netmask 255.255.255.240
# route add default gw 192.168.0.1
# ping 192.168.0.1
# ping 172.16.80.1
# ping www.cict.fr
```

¹⁰ <http://www.linux-france.org/prj/inetdoc/cours/config.interface/>