

Synthèse sur le service DNS

Philippe Latu

philippe.latu(at)linux-france.org

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

Historique des versions		
\$Revision: 1619 \$	\$Date: 2011-04-05 00:08:00 +0200 (mar. 05 avril 2011) \$	\$Author: latu \$
Année universitaire 2009-2010		
Résumé		
À la suite des séances de travaux pratiques consacrées à l'étude du Domain Name System (DNS), voici une synthèse reprenant les opérations de configuration et de test à effectuer lors de la mise en oeuvre de ce service.		

Table des matières

1. Copyright et Licence	2
1.1. Meta-information	2
1.2. Conventions typographiques	2
2. Architecture type de travaux pratiques	3
3. Installation du service DNS cache-only	3
4. Requêtes DNS sur les différents types d'enregistrements (<i>Resource Records</i>)	6
4.1. Types de la classe Internet (IN)	6
4.2. Types de la classe CHAOS	9
4.3. Validation ou dépannage d'une configuration	10
5. Configuration du serveur primaire de la zone stri.lab	13
6. Configuration du serveur secondaire de la zone stri.lab	15
7. Délégation de la zone stri.lab depuis le niveau lab	17
8. Sécurisation de premier niveau	20
9. Documents de référence	22

1. Copyright et Licence

Copyright (c) 2000,2011 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) 2000,2011 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 1.2 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.

1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou *prompt* spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite `$` ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite `#` nécessite les privilèges du super-utilisateur.

¹ <http://www.docbook.org>

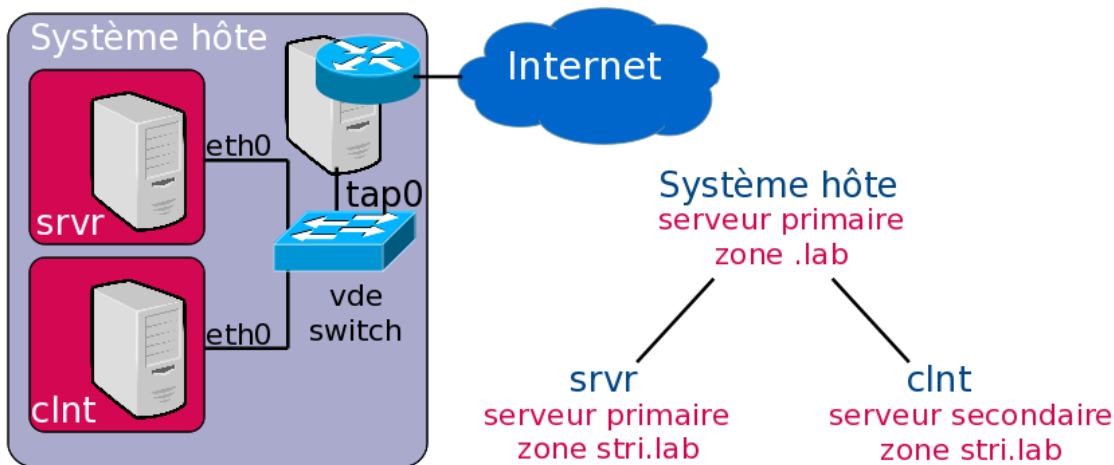
² <http://www.debian.org>

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 *Architecture réseau des travaux pratiques*⁵, on part d'une configuration type avec deux de postes de travail qui partagent le même domaine de diffusion. Le schéma d'une maquette utilisant deux instances de machines virtuelles et un système hôte est le suivant :



Topologie synthèse DNS - vue complète⁶

Tableau 1. Plan d'adressage IP

	srvr	clnt	système hôte
Adresse primaire	192.200.0.3/27	192.200.0.4/27	192.200.0.1/27
Adresse secondaire service SMTP	192.200.0.10/27		
Adresse secondaire service NFS	192.200.0.11/27		
Adresse secondaire service LDAP		192.200.0.12/27	

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 de la distribution vers la chaîne de caractères qui débute par "bind".

```
$ aptitude search ?name"(^bind)"
p  bind9          - Internet Domain Name Server
p  bind9-doc      - Documentation for BIND
i  bind9-host    - Version of 'host' bundled with BIND 9.X
p  bind9utils    - Utilities for BIND
p  bindfs        - mirrors or overlays a local directory with altered permissions
p  bindgraph     - DNS statistics RRDtool frontend for BIND9
```

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

```
$ aptitude search ~ibind9
i  bind9          - Internet Domain Name Server
i  bind9-doc      - Documentation for BIND
i  bind9-host    - Version of 'host' bundled with BIND 9.X
i  A bind9utils  - Utilities for BIND
i  libbind9-60   - BIND9 Shared Library used by BIND
```

⁵ <http://www.linux-france.org/prj/inetdoc/cours/archi.tp/>

⁶ <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.synthese-dns/images/synthese-dns.png>


```
# dpkg -L bind9 |grep etc
/etc
/etc/init.d
/etc/init.d/bind9
/etc/network
/etc/network/if-down.d
/etc/network/if-down.d/bind9
/etc/network/if-up.d
/etc/network/if-up.d/bind9
/etc/ppp
/etc/ppp/ip-up.d
/etc/ppp/ip-up.d/bind9
/etc/ppp/ip-down.d
/etc/ppp/ip-down.d/bind9
/etc/ufw
/etc/ufw/applications.d
/etc/ufw/applications.d/bind9
/etc/bind
/etc/bind/named.conf.default-zones
/etc/bind/named.conf
/etc/bind/zones.rfc1918
/etc/bind/db.127
/etc/bind/db.root
/etc/bind/db.255
/etc/bind/bind.keys
/etc/bind/db.empty
/etc/bind/named.conf.local
/etc/bind/named.conf.options
/etc/bind/db.local
/etc/bind/db.0
/etc/apparmor.d
/etc/apparmor.d/force-complain
/etc/apparmor.d/usr.sbin.named
```

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

```
# dpkg -L bind9 |grep var
/var
/var/cache
/var/cache/bind
/var/run
/var/run/named
```

C'est dans le répertoire `/var/cache/bind/` que l'on place les fichiers contenant les enregistrements ou *Resource Records* (RRs). Ces enregistrements correspondent aux zones sur lesquelles le serveur a autorité. Ce choix de répertoire fait partie des options du service. Voir l'option `directory` dans le fichier `/etc/bind/named.conf.options`.

L'installation par défaut du paquet de la distribution fournit une configuration de type *cache-only* :

- Il ne contient aucune déclaration de zone. Le fichier `/etc/bind/named.conf.local` ne contient que des commentaires.
- Le répertoire `/var/cache/bind/` est vide.
- Le service peut contacter les serveurs racine. La liste de ces serveurs est donnée dans le fichier `db.root`.
- Le service étant actif, il peut prendre en charge les requêtes et mémoriser dans son cache les résultats.

Vu du système sur lequel le service est exécuté, on optimise le traitement des requêtes en alimentant puis en utilisant le cache mémoire. Vu de l'Internet, on surcharge les serveurs racines en les sollicitant directement à chaque nouvelle requête.

C'est le fichier `/etc/resolv.conf` qui sert à configurer la partie client du service de résolution des noms ; le *resolver*. Dans le cas des postes de travaux pratiques, la configuration initiale du *resolver* est prise en charge par le service DHCP.

On doit éditer le fichier `/etc/resolv.conf` pour qu'il fasse référence au service de résolution des noms installé sur le système.

```
# cat /etc/resolv.conf
```

```
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 :

```
# 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 d'enregistrements (*Resource Records*)

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 700ms tandis que la seconde a un temps de traitement de 0ms. Cette seconde réponse est fournie par le cache du serveur DNS.

```
# dig www.linux-france.org
<snipped/>
;; Query time: 700 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 13:16:14 2010
;; MSG SIZE rcvd: 177
```

```
# dig www.linux-france.org
<snipped/>
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 13:19:04 2010
;; MSG SIZE rcvd: 177
```

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

```
$ dig nic.fr ns

; <<>> DiG 9.7.0-P1 <<>> nic.fr ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9644
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
nic.fr.      172800  IN      NS      ns3.nic.fr.
nic.fr.      172800  IN      NS      ns2.ext.nic.fr.
nic.fr.      172800  IN      NS      ns1.ext.nic.fr.
nic.fr.      172800  IN      NS      ns4.ext.nic.fr.
nic.fr.      172800  IN      NS      ns3.ext.nic.fr.
nic.fr.      172800  IN      NS      ns1.nic.fr.
nic.fr.      172800  IN      NS      ns2.nic.fr.

;; Query time: 201 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 11:25:14 2010
```

```
;; MSG SIZE rcvd: 154
```

Requête sur un nom d'hôte, A

```
$ dig www.nic.fr

; <<>> DiG 9.7.0-P1 <<>> www.nic.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20692
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.nic.fr.                172800 IN      CNAME  rigolo.nic.fr.
rigolo.nic.fr.            172800 IN      A      192.134.4.20

;; AUTHORITY SECTION:
nic.fr.                    172626 IN      NS      ns4.ext.nic.fr.
nic.fr.                    172626 IN      NS      ns2.ext.nic.fr.
nic.fr.                    172626 IN      NS      ns1.nic.fr.
nic.fr.                    172626 IN      NS      ns3.ext.nic.fr.
nic.fr.                    172626 IN      NS      ns1.ext.nic.fr.
nic.fr.                    172626 IN      NS      ns3.nic.fr.
nic.fr.                    172626 IN      NS      ns2.nic.fr.

;; Query time: 134 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 11:28:08 2010
;; MSG SIZE rcvd: 195
```

Requête sur une adresse IP, PTR

```
$ dig -x 192.134.4.20

; <<>> DiG 9.7.0-P1 <<>> -x 192.134.4.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31468
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, 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.

;; AUTHORITY SECTION:
4.134.192.in-addr.arpa. 172800 IN      NS      ns2.nic.fr.
4.134.192.in-addr.arpa. 172800 IN      NS      ns1.nic.fr.
4.134.192.in-addr.arpa. 172800 IN      NS      ns3.nic.fr.

;; Query time: 912 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 11:29:35 2010
;; MSG SIZE rcvd: 124
```

Requête sur un agent de transfert de courrier électronique, MX

```
$ dig nic.fr mx

; <<>> DiG 9.7.0-P1 <<>> nic.fr mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59170
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 7, ADDITIONAL: 5

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

```

;; ANSWER SECTION:
nic.fr.          172800  IN      MX      20 mx2.nic.fr.
nic.fr.          172800  IN      MX      30 mx3.nic.fr.
nic.fr.          172800  IN      MX      10 mx1.nic.fr.

;; AUTHORITY SECTION:
nic.fr.          172442  IN      NS      ns2.ext.nic.fr.
nic.fr.          172442  IN      NS      ns1.nic.fr.
nic.fr.          172442  IN      NS      ns3.ext.nic.fr.
nic.fr.          172442  IN      NS      ns1.ext.nic.fr.
nic.fr.          172442  IN      NS      ns3.nic.fr.
nic.fr.          172442  IN      NS      ns2.nic.fr.
nic.fr.          172442  IN      NS      ns4.ext.nic.fr.

;; ADDITIONAL SECTION:
mx1.nic.fr.     172800  IN      A       192.134.4.10
mx1.nic.fr.     172800  IN      AAAA    2001:660:3003:2::4:10
mx2.nic.fr.     172800  IN      A       192.134.4.11
mx2.nic.fr.     172800  IN      AAAA    2001:660:3003:2::4:11
mx3.nic.fr.     172800  IN      A       192.134.4.11

;; Query time: 97 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 11:31:12 2010
;; MSG SIZE rcvd: 318

```

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

```

$ dig +trace www.nic.fr

; <<>> DiG 9.7.0-P1 <<>> +trace www.nic.fr
;; global options: +cmd
.           524366  IN      NS      f.root-servers.net.
.           524366  IN      NS      j.root-servers.net.
.           524366  IN      NS      k.root-servers.net.
.           524366  IN      NS      m.root-servers.net.
.           524366  IN      NS      i.root-servers.net.
.           524366  IN      NS      c.root-servers.net.
.           524366  IN      NS      b.root-servers.net.
.           524366  IN      NS      h.root-servers.net.
.           524366  IN      NS      d.root-servers.net.
.           524366  IN      NS      g.root-servers.net.
.           524366  IN      NS      l.root-servers.net.
.           524366  IN      NS      e.root-servers.net.
.           524366  IN      NS      a.root-servers.net.
;; Received 500 bytes from 127.0.0.1#53(127.0.0.1) in 0 ms

fr.         172800  IN      NS      a.nic.fr.
fr.         172800  IN      NS      c.nic.fr.
fr.         172800  IN      NS      d.ext.nic.fr.
fr.         172800  IN      NS      d.nic.fr.
fr.         172800  IN      NS      e.ext.nic.fr.
fr.         172800  IN      NS      f.ext.nic.fr.
fr.         172800  IN      NS      g.ext.nic.fr.
;; Received 430 bytes from 128.63.2.53#53(h.root-servers.net) in 144 ms

nic.fr.     172800  IN      NS      ns2.nic.fr.
nic.fr.     172800  IN      NS      ns1.ext.nic.fr.
nic.fr.     172800  IN      NS      ns3.nic.fr.
nic.fr.     172800  IN      NS      ns3.ext.nic.fr.
nic.fr.     172800  IN      NS      ns2.ext.nic.fr.
nic.fr.     172800  IN      NS      ns1.nic.fr.
nic.fr.     172800  IN      NS      ns4.ext.nic.fr.
;; Received 382 bytes from 193.176.144.6#53(e.ext.nic.fr) in 224 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      ns4.ext.nic.fr.
nic.fr.     172800  IN      NS      ns2.ext.nic.fr.
nic.fr.     172800  IN      NS      ns3.ext.nic.fr.

```

```

nic.fr.          172800 IN      NS       ns1.nic.fr.
nic.fr.          172800 IN      NS       ns2.nic.fr.
nic.fr.          172800 IN      NS       ns1.ext.nic.fr.
nic.fr.          172800 IN      NS       ns3.nic.fr.
;; Received 419 bytes from 192.134.0.49#53(ns3.nic.fr) in 57 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 alimenter 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. Les contrôles d'accès qui permettent de ne satisfaire que les requêtes émises par les hôtes appartenant aux «réseaux de confiance» sont présentées dans la [Section 8, «Sécurisation de premier niveau»](#).

4.2. Types de la classe CHAOS

Tous 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 souvent recherchés : la version du logiciel et la liste de ses auteurs.

```

$ dig @localhost. version.bind txt chaos +novc

; <<>> DiG 9.7.0-P1 <<>> @localhost. version.bind txt chaos +novc
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4759
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
version.bind.          0      CH      TXT      "9.7.0-P1"

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

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Mon May 24 11:35:57 2010
;; MSG SIZE rcvd: 65

```

```

$ dig @localhost. authors.bind txt chaos +novc

; <<>> DiG 9.7.0-P1 <<>> @localhost. authors.bind txt chaos +novc
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21420
;; flags: qr aa rd; QUERY: 1, ANSWER: 14, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
authors.bind.          0      CH      TXT      "Jeremy C. Reed"
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      "Evan Hunt"

```

```

authors.bind.      0      CH      TXT      "David Lawrence"
authors.bind.      0      CH      TXT      "Danny Mayer"
authors.bind.      0      CH      TXT      "Damien Neil"
authors.bind.      0      CH      TXT      "Matt Nelson"

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

;; Query time: 4 msec
;; SERVER: ::1#53(::1)
;; WHEN: Mon May 24 11:38:55 2010
;; MSG SIZE rcvd: 404

```

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.

4.3. Validation ou dépannage d'une configuration

Les sections précédentes sur les types de requêtes fournissent déjà quelques éléments sur la validation ou le dépannage du service DNS.

- Le temps de réponse à une requête (*Query time:*) renseigne sur l'utilisation ou non du cache mémoire.
- En cas de panne, une **requête itérative** permet d'identifier le point de rupture dans la chaîne de résolution des noms.

Il reste deux options particulièrement utiles à la mise au point d'une configuration correcte.

Il est possible de désigner explicitement le serveur DNS qui doit prendre en charge la requête à l'aide de son adresse IP. Cette opération est très utile pour vérifier qu'un serveur primaire répond correctement aux demandes sur les enregistrements qu'il détient. Dans le contexte de la sécurisation du service, cette même opération sert à contrôler qu'un serveur ne répond qu'au requêtes qu'il est sensé traiter. Voici deux exemples utilisant respectivement la désignation du serveur interrogé par son adresse IP et la requête directe de transfert de zone.

Pour vérifier que le service DNS de la zone `nic.fr` fournit l'adresse du serveur Web ayant le nom `www.nic.fr`, on peut procéder comme suit.

- On identifie un serveur de nom pour la zone.

```

$ dig nic.fr ns

; <<>> DiG 9.7.0-P1 <<>> nic.fr ns
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 59555
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
nic.fr.                IN      NS

;; ANSWER SECTION:
nic.fr.                172554 IN      NS      ns1.nic.fr.
nic.fr.                172554 IN      NS      ns4.ext.nic.fr.
nic.fr.                172554 IN      NS      ns3.ext.nic.fr.
nic.fr.                172554 IN      NS      ns2.nic.fr.
nic.fr.                172554 IN      NS      ns2.ext.nic.fr.
nic.fr.                172554 IN      NS      ns3.nic.fr.
nic.fr.                172554 IN      NS      ns1.ext.nic.fr.

;; ADDITIONAL SECTION:
ns1.nic.fr.           172570 IN      A       192.93.0.1
ns1.nic.fr.           172570 IN      AAAA    2001:660:3005:1::1:1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 19:05:15 2010

```

```
;; MSG SIZE rcvd: 198
```

- On interroge directement le serveur primaire de la zone.

```
$ dig @ns1.nic.fr. www.nic.fr

; <<>> DiG 9.7.0-P1 <<>> @ns1.nic.fr. www.nic.fr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18931
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 11
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
www.nic.fr.                172800 IN      CNAME  rigolo.nic.fr.
rigolo.nic.fr.            172800 IN      A      192.134.4.20

;; AUTHORITY SECTION:
nic.fr.                    172800 IN      NS      ns2.nic.fr.
nic.fr.                    172800 IN      NS      ns1.ext.nic.fr.
nic.fr.                    172800 IN      NS      ns2.ext.nic.fr.
nic.fr.                    172800 IN      NS      ns1.nic.fr.
nic.fr.                    172800 IN      NS      ns3.nic.fr.
nic.fr.                    172800 IN      NS      ns3.ext.nic.fr.
nic.fr.                    172800 IN      NS      ns4.ext.nic.fr.

;; ADDITIONAL SECTION:
ns1.ext.nic.fr.           172800 IN      A      193.51.208.13
ns1.nic.fr.              172800 IN      A      192.93.0.1
ns1.nic.fr.              172800 IN      AAAA   2001:660:3005:1::1:1
ns2.ext.nic.fr.          172800 IN      A      194.2.0.30
ns2.nic.fr.              172800 IN      A      192.93.0.4
ns2.nic.fr.              172800 IN      AAAA   2001:660:3005:1::1:2
ns3.ext.nic.fr.          172800 IN      A      194.2.0.60
ns3.nic.fr.              172800 IN      A      192.134.0.49
ns3.nic.fr.              172800 IN      AAAA   2001:660:3006:1::1:1
ns4.ext.nic.fr.          172800 IN      A      193.0.0.196
ns4.ext.nic.fr.          172800 IN      AAAA   2001:610:240:0:53::4

;; Query time: 77 msec
;; SERVER: 192.93.0.1#53(192.93.0.1)
;; WHEN: Mon May 24 19:08:52 2010
;; MSG SIZE rcvd: 419
```

On voit apparaître une indication selon laquelle le serveur interrogé ne prendra pas en charge les requêtes récursives pour le client utilisé. C'est tout à fait normal dans la mesure où ces tests de requêtes ne sont pas effectués depuis un poste client appartenant au domaine `nic.fr`.

Pour autant, on obtient bien la réponse à la requête posée puisque l'enregistrement demandé appartient bien à la zone sur laquelle le serveur a autorité.

- On interroge directement le même serveur avec une requête portant sur une autre zone.

```
$ dig @ns1.nic.fr. www.laredoute.fr

; <<>> DiG 9.7.0-P1 <<>> @ns1.nic.fr. www.laredoute.fr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 15319
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; Query time: 74 msec
```

```
;; SERVER: 192.93.0.1#53(192.93.0.1)
;; WHEN: Mon May 24 19:16:10 2010
;; MSG SIZE rcvd: 34
```

Cette fois-ci la requête est refusée. Le serveur primaire ne veut pas prendre en charge la requête posée. C'est encore tout à fait normal dans la mesure le client n'appartient pas aux réseaux de la zone `nic.fr`.

- Certains services sont très «ouverts» et acceptent de prendre en charge les requêtes de n'importe quel client. La même requête posée à un de ces services est traitée normalement.

```
$ dig @dns2.gaoland.net. www.laredoute.fr

; <<>> DiG 9.7.0-P1 <<>> @dns2.gaoland.net. www.laredoute.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11454
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 9, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.laredoute.fr.                1800    IN      CNAME   laredoute.fr.edgekey.net.
laredoute.fr.edgekey.net.        3415    IN      CNAME   e143.b.akamaiedge.net.
e143.b.akamaiedge.net.          20      IN      A       88.221.192.169

;; AUTHORITY SECTION:
b.akamaiedge.net.                1566    IN      NS      n0b.akamaiedge.net.
b.akamaiedge.net.                2466    IN      NS      n1b.akamaiedge.net.
b.akamaiedge.net.                3366    IN      NS      n5b.akamaiedge.net.
b.akamaiedge.net.                2466    IN      NS      n7b.akamaiedge.net.
b.akamaiedge.net.                2466    IN      NS      n4b.akamaiedge.net.
b.akamaiedge.net.                3366    IN      NS      n8b.akamaiedge.net.
b.akamaiedge.net.                1566    IN      NS      n3b.akamaiedge.net.
b.akamaiedge.net.                3366    IN      NS      n2b.akamaiedge.net.
b.akamaiedge.net.                1566    IN      NS      n6b.akamaiedge.net.

;; ADDITIONAL SECTION:
n0b.akamaiedge.net.              1566    IN      A       81.52.251.5
n1b.akamaiedge.net.              1717    IN      A       213.200.111.69
n5b.akamaiedge.net.              3366    IN      A       81.52.251.8
n7b.akamaiedge.net.              1717    IN      A       81.52.251.13
n4b.akamaiedge.net.              1717    IN      A       81.52.251.12
n8b.akamaiedge.net.              3366    IN      A       81.52.251.5
n3b.akamaiedge.net.              1566    IN      A       81.52.251.9
n2b.akamaiedge.net.              3366    IN      A       80.239.234.150
n6b.akamaiedge.net.              1566    IN      A       81.52.251.18

;; Query time: 74 msec
;; SERVER: 212.94.162.33#53(212.94.162.33)
;; WHEN: Mon May 24 19:19:22 2010
;; MSG SIZE rcvd: 442
```

Sous toute réserve, il semble bien que le fait de répondre aux requêtes de n'importe quel client ne corresponde pas aux bonnes pratiques sur la configuration du service DNS de nos jours.

Dans le cadre de ces travaux pratiques, on veillera donc à n'autoriser les requêtes récursives qu'aux clients appartenant aux réseaux définis dans le plan d'adressage IP de l'énoncé.

La requête directe de transfert de zone permet de valider les autorisations d'échanges entre le serveur primaire et les autres serveurs ayant autorité sur la même zone.

Dans l'exemple de requête ci-dessous on interroge le serveur primaire à partir du serveur secondaire.

```
# dig @ns.stri.lab stri.lab axfr

; <<>> DiG 9.7.0-P1 <<>> @ns.stri.lab stri.lab axfr
; (1 server found)
;; global options: +cmd
```

```

stri.lab.      60      IN      SOA      stri.lab. root.stri.lab. 2010052401 20 5 420 60
stri.lab.      60      IN      TXT      "Training Lab"
stri.lab.      60      IN      MX       10 smtp.stri.lab.
stri.lab.      60      IN      NS       clnt.stri.lab.
stri.lab.      60      IN      NS       srvr.stri.lab.
clnt.stri.lab. 60      IN      A        192.200.0.4
ldap.stri.lab. 60      IN      A        192.200.0.12
nfs.stri.lab.  60      IN      A        192.200.0.11
ns1.stri.lab.  60      IN      CNAME    srvr.stri.lab.
ns2.stri.lab.  60      IN      CNAME    clnt.stri.lab.
rtr.stri.lab.  60      IN      A        192.200.0.1
smtp.stri.lab. 60      IN      A        192.200.0.10
srvr.stri.lab. 60      IN      A        192.200.0.3
stri.lab.      60      IN      SOA      stri.lab. root.stri.lab. 2010052401 20 5 420 60
;; Query time: 2 msec
;; SERVER: 192.200.0.3#53(192.200.0.3)
;; WHEN: Mon May 24 17:51:00 2010
;; XFR size: 14 records (messages 1, bytes 332)

```

Pour éviter une «recensement trop facile» de l'identité des hôtes d'une zone, il est essentiel de n'autoriser ces requêtes de transfert qu'entre serveurs DNS. Cette configuration du contrôle d'accès est présentée dans la [Section 8, « Sécurité de premier niveau »](#).

5. Configuration du serveur primaire de la zone stri.lab

Le fichier `/etc/bind/named.conf.local` du nouveau serveur DNS doit être édité. Une fois l'opération effectuée, le serveur a autorité sur la zone `stri.lab`. Voici une copie de ce fichier.

```

# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

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

zone "0.200.192.in-addr.arpa" {
    type master;
    file "192.200.0";
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

```

En respectant les options de configuration du paquet Debian, on crée les fichiers `stri.lab` et `192.200.0` dans le répertoire `/var/cache/bind/`.

- Enregistrements (RRs) utilisés pour la résolution directe des noms.

```

# cat /var/cache/bind/stri.lab
$TTL 60
@      IN      SOA      stri.lab. root.stri.lab. (
                2010052401      ; serial, yearmonthdayserial#
                20                ; refresh, seconds
                5                 ; retry, seconds
                420               ; expire, seconds
                60 )              ; minimum, seconds
NS     srvr.stri.lab.
NS     clnt.stri.lab.
MX     10 smtp.stri.lab. ; Primary Mail Exchanger
TXT    "Training Lab"

rtr    A        192.200.0.1
srvr   A        192.200.0.3
ns1    CNAME    srvr.stri.lab.
clnt   A        192.200.0.4

```



```

named[1307]: zone stri.lab/IN: loaded serial 2010052401
named[1307]: zone localhost/IN: loaded serial 2
named[1307]: running
named[1307]: zone 0.200.192.in-addr.arpa/IN: sending notifies (serial 2010052401)
named[1307]: zone stri.lab/IN: sending notifies (serial 2010052401)

```

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.

```

# dig stri.lab ns

; <<>> DiG 9.7.0-P1 <<>> stri.lab ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59703
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
stri.lab.                IN      NS

;; ANSWER SECTION:
stri.lab.                60      IN      NS      clnt.stri.lab.
stri.lab.                60      IN      NS      srvr.stri.lab.

;; ADDITIONAL SECTION:
clnt.stri.lab.          60      IN      A       192.200.0.4
srvr.stri.lab.          60      IN      A       192.200.0.3

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 24 16:57:00 2010
;; MSG SIZE rcvd: 96

```

Comme dans l'exemple ci-dessus, on peut valider 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 d'enregistrements \(*Resource Records*\) »](#).

6. Configuration du serveur secondaire de la zone stri.lab

Pour distinguer un serveur primaire d'un serveur secondaire, il faut savoir que le serveur primaire détient effectivement les fichiers de déclaration des enregistrements. Un serveur secondaire obtient les copies des déclarations des enregistrements par transfert réseau.

Dans cette section, on reprend les mêmes fichiers de configuration en désignant le serveur primaire comme détenteur des enregistrements.

Le fichier `/etc/bind/named.conf.local` du nouveau serveur DNS doit être édité. Une fois l'opération effectuée, le serveur a autorité sur la zone `stri.lab`. Voici une copie de ce fichier.

```

# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "stri.lab" {
    type slave;
    masters {
        192.200.0.3;
    };
    file "backup.stri.lab";
};

zone "0.200.192.in-addr.arpa" {
    type slave;
    masters {
        192.200.0.3;
    };
    file "backup.192.200.0";
};

```



```

NS      srvr.stri.lab.
MX      10 smtp.stri.lab.
TXT     "Training Lab"
$ORIGIN stri.lab.
clnt    A      192.200.0.4
ldap    A      192.200.0.12
nfs     A      192.200.0.11
ns1     CNAME  srvr
ns2     CNAME  clnt
rtr     A      192.200.0.1
smtp    A      192.200.0.10
srvr    A      192.200.0.3

```

Comme dans la section précédente, on peut valider un à un les enregistrements en interrogeant le service. Voici juste un exemple désignant explicitement le serveur secondaire.

```

# dig @192.200.0.4 stri.lab mx

; <<>> DiG 9.7.0-P1 <<>> @192.200.0.4 stri.lab mx
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29883
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
stri.lab.                IN      MX

;; ANSWER SECTION:
stri.lab.                60      IN      MX      10 smtp.stri.lab.

;; AUTHORITY SECTION:
stri.lab.                60      IN      NS      srvr.stri.lab.
stri.lab.                60      IN      NS      clnt.stri.lab.

;; ADDITIONAL SECTION:
smtp.stri.lab.           60      IN      A      192.200.0.10
clnt.stri.lab.           60      IN      A      192.200.0.4
srvr.stri.lab.           60      IN      A      192.200.0.3

;; Query time: 0 msec
;; SERVER: 192.200.0.4#53(192.200.0.4)
;; WHEN: Mon May 24 16:24:53 2010
;; MSG SIZE rcvd: 133

```

Lors d'une modification de la liste des enregistrements, il est important d'incrémenter correctement le numéro de série de façon à notifier l'ensemble des serveurs ayant autorité sur une zone. Dans l'extrait du fichier `/var/log/syslog/` du serveur primaire donné ci-dessous, on voit bien apparaître ces notifications.

```

named[1556]: running
named[1556]: zone 0.200.192.in-addr.arpa/IN: sending notifies (serial 2010052402)
named[1556]: zone stri.lab/IN: sending notifies (serial 2010052402)
named[1556]: client 192.200.0.4#41748: transfer of '0.200.192.in-addr.arpa/IN': AXFR-style IXFR started
named[1556]: client 192.200.0.4#41748: transfer of '0.200.192.in-addr.arpa/IN': AXFR-style IXFR ended
named[1556]: client 192.200.0.4#19941: received notify for zone '0.200.192.in-addr.arpa'
named[1556]: client 192.200.0.4#40869: transfer of 'stri.lab/IN': AXFR-style IXFR started
named[1556]: client 192.200.0.4#40869: transfer of 'stri.lab/IN': AXFR-style IXFR ended
named[1556]: client 192.200.0.4#2069: received notify for zone 'stri.lab'

```

7. Délégation de la zone stri.lab depuis le niveau lab



Avertissement

Cette partie est complétée par l'enseignant sur le serveur DNS de travaux pratiques ayant autorité au niveau supérieur ; ce niveau supérieur correspond à un *Top Level Domain* (TLD) factice.

Le serveur maître de la zone `lab` doit *déléguer* le domaine `stri.lab` aux postes de travaux pratiques qui détiennent les enregistrements (RRs) du sous-domaine.

Dans le contexte de la **maquette utilisée pour ce document**, le système hôte doit déléguer le sous-domaine aux deux instances de machines virtuelles.

Les fichiers de configuration donnés dans cette section sont surtout utiles pour les communications inter-zones lors des travaux pratiques. En effet, pour que les services internet qui s'appuient sur la résolution des noms puissent fonctionner normalement, il est essentiel que les branches de cette arborescence DNS factice soient toutes reliées les unes aux autres.

Le fichier de déclaration de zone du système hôte se présente comme suit.

```
# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "lab" {
    type master;
    file "lab";
    notify no;
};

zone "16/200.192.in-addr.arpa" {
    type master;
    file "192.200";
    notify no;
};

zone "stri.lab" {
    type slave;
    file "backup.stri.lab";
    masters {
        192.200.0.3;
        192.200.0.4;
    };
};

zone "0.200.192.in-addr.arpa" {
    type slave;
    file "backup.192.200.0";
    masters {
        192.200.0.3;
        192.200.0.4;
    };
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

Les deux fichiers désignés pour contenir les définitions des enregistrements sont donnés ci-dessous.

- Enregistrements pour la résolution des noms.

```
# cat /var/cache/bind/lab
$TTL 60
@      IN      SOA      lab. root.lab. (
                        2010052401      ; serial, yearmonthdayserial#
                        20                ; refresh, seconds
                        5                 ; retry, seconds
                        420               ; expire, seconds
                        60 )              ; minimum, seconds
      NS      host-srvr.lab.
      MX      10 smtp.lab. ; Primary Mail Exchanger
      TXT     "Training Lab Host System"

host-srvr    A      192.200.0.1
smtp         A      192.200.0.2
vm-srvr      A      192.200.0.3
vm-clnt      A      192.200.0.4
```

- Enregistrements pour la résolution inverse des adresses IP.


```
named[13597]: zone 0.200.192.in-addr.arpa/IN: sending notifies (serial 2010052402)
named[13597]: zone stri.lab/IN: sending notifies (serial 2010052402)
named[13597]: running
```

On peut vérifier que les numéros de série des notifications correspondent bien aux enregistrements publiés au niveau inférieur.

Pour clore la validation de la délégation, il faut reprendre la série de tests de requêtes présentées dans les deux sections précédentes.

8. Sécurisation de premier niveau

L'objectif de cette section est de présenter les mécanismes de contrôle d'accès offerts par le service *Berkeley Internet Name Domain* à un niveau très modeste. On se contente ici de définir les adresses IP ou les réseaux qui sont autorisés à émettre des requêtes récursives sur le service DNS ainsi que les adresses IP ou les réseaux qui sont autorisés à émettre des requêtes de transfert de zone.

Les éléments de configuration présentés ci-après sont à appliquer sur tous les serveurs DNS quel que soit leur rôle.

On commence par la définition des listes de contrôle d'accès dans le fichier `/etc/bind/named.conf.options`. Ces listes permettent de définir des groupes d'adresses IP ou de réseaux. Ces groupes peuvent ensuite être réutilisés autant de fois que nécessaire au niveau global de la configuration du service ou bien dans les déclarations de zones.

Ici, on se limite à la définition de deux groupes.

- Le groupe `xfer` donne la liste des adresses IP à partir desquelles les opérations de transfert de zone sont possibles.
- Le groupe `trusted` donne la liste des réseaux de confiance qui sont habilités à utiliser le service.

Ces définitions se retrouvent au début du fichier de configuration global du service DNS.

```
# cat /etc/bind/named.conf.options
acl "xfer" {
    localhost;
    192.200.0.1;
    192.200.0.3;
    192.200.0.4;
};

acl "trusted" {
    localhost;
    192.200.0.0/27;
};

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        192.200.0.1;
    };

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };

    allow-transfer {
        none;
    };

    allow-query {
```

```

trusted;
};

allow-query-cache {
  trusted;
};
};

```

C'est dans la section `options` que l'on trouve la première utilisation des listes de contrôle d'accès. Ce niveau est dit global puisqu'il est examiné avant les déclarations de zone qui sont effectuées dans le fichier `/etc/bind/named.conf.local`. Dans l'exemple donné ci-dessus, les opérations de transfert sont interdites au niveau global et les requêtes récursives pour des enregistrements sur lesquels le serveur n'a pas autorité ne sont autorisées que pour les réseaux de confiance.

Il faut noter que la section `forwarders` a été décommentée et configurée avec l'adresse IP du serveur de niveau supérieur dans l'arborescence DNS. Cette configuration est nécessaire pour garantir la «continuité» de l'arborescence factice de travaux pratiques. Il faut que les communications inter zones soient effectives pour mettre en œuvre les autres services internet qui s'appuient sur la résolution des noms.

On retrouve les listes de contrôle d'accès dans le fichier de déclaration de zone.

```

# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "0.200.192.in-addr.arpa" {
    type master;
    file "192.200.0";

    allow-query {
        any;
    };

    allow-transfer {
        xfer;
    };
};

zone "stri.lab" {
    type master;
    file "stri.lab";

    allow-query {
        any;
    };

    allow-transfer {
        xfer;
    };
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

```

Les choix effectués ici reviennent à autoriser sans restriction les requêtes directes et inverses sur les enregistrements de la zone `stri.lab`. Les transferts sur les mêmes enregistrements ne sont autorisés que pour les serveurs dont les adresses IP figurent dans la liste `xfer`.

Comme dans les sections précédentes, ces options de configuration sont à valider avec la suite des tests utilisant les différents types de requêtes à l'aide de la commande **dig**. À titre d'exemple, voici ce que l'on peut lire dans les journaux système lors d'une requête de transfert de zone non autorisée.

```

named[1524]: client 192.200.0.4#58025: zone transfer 'stri.lab/AXFR/IN' denied

```

Pour être plus complète, la sécurisation de la configuration devrait utiliser la notion de vue interne et externe du service de résolution des noms. Ce niveau de configuration dépasse «quelque peu» le cadre de ces travaux pratiques

d'introduction. Le contenu de cette section n'est qu'une première prise de contact avec les fonctionnalités de sécurité d'un serveur DNS.

9. Documents de référence

BIND 9 Administrator Reference Manual

*BIND 9 Administrator Reference Manual*⁸ : 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*⁹ : documentation complète sur la configuration serveur et client DNS.

Secure BIND Template

*Secure BIND Template*¹⁰ : patrons de fichiers de configuration d'un service DNS.

Administration système en réseau : architecture réseau

*Architecture réseau des travaux pratiques*¹¹ : présentation de l'infrastructure des travaux pratiques.

Configuration d'une interface de réseau local

*Configuration d'une interface de réseau local*¹² : tout sur la configuration des interfaces réseau ; notamment les 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
```

⁸ <http://www.bind9.net/manuals>

⁹ <http://www.tldp.org/HOWTO/DNS-HOWTO.html>

¹⁰ <http://www.cymru.com/Documents/secure-bind-template.html>

¹¹ <http://www.linux-france.org/prj/inetdoc/cours/archi.tp/>

¹² <http://www.linux-france.org/prj/inetdoc/cours/config.interface.lan/>