

Configuració del servei DNS

Eduard Canet i Ricart

Índex

Índex.....	2
1. El servei DNS	3
a) Comprendre el funcionament general del protocol DNS	5
1. Fer la llista dels ports.....	5
2. Monitorar el trànsit UDP del protocol DNS.....	5
Utilitat <i>iptraf</i>	5
Utilitat <i>nmap</i>	6
3 Monitorar el trànsit de xarxa amb el Wireshark	7
4 Consultes amb <i>dig</i> , <i>nslookup</i> i <i>hoste</i>	7
Utilitat <i>dig</i>	7
Utilitat <i>nslookup</i>	9
Utilitat <i>hoste</i>	12
5. Consultar la configuració del client: sistema de resolució	12
b) Instal·lar i configurar un servidor DNS.....	14
1. Instal·lar el servidor DNS i observar-ne els components.....	14
Instal·lar el programari servidor	14
Observar els components del paquet.....	15
Resum	18
2. Activar o desactivar el servei i establir els nivells d'arrencada....	18
El servei	18
Estat del servei.....	19
Establir els nivells del servei per defecte	19
3. Monitorar les activitats del servidor i del procés	21
Els fitxers de registre	21
El procés del servei.....	21
La concurrència	21
4. Configuració del servei DNS	22
Configuració bàsica.....	22
Exemple de configuració bàsica	25
5. Monitorar el trànsit amb el Wireshark.....	27
Monitoratge	¡Error! Marcador no definido.

1. El servei DNS

En aquesta activitat l'estudiant aprendrà a utilitzar el servei DNS (*domain name server*, servidor de noms de domini). Primerament ha d'entendre el funcionament general del servei de noms de domini i la manera de cercar informació. També ha de conèixer les diverses eines client que permeten fer consultes DNS. Finalment ha de ser capaç d'instal·lar i configurar un servidor DNS per a un domini local per proporcionar el servei de noms als equips del domini local.

Per dur a terme cada una d'aquestes accions dividim l'apartat en dos blocs; el primer per tractar el protocol en si i el segon per treballar-lo com a servidor. Es tracta de fer el següent:

a) Comprendre el funcionament general del protocol DNS

1. Fer la llista dels ports utilitzats pel protocol DNS del fitxer amb la llista de ports d'un sistema GNU/Linux (habitualment, */etc/services*).
2. Utilitzar les ordres de monitoratge del trànsit UDP (normalment, *nmap*, *netstat*, *ss* i *iptraf*, entre d'altres) per observar els ports oberts en el client i en el servidor.
3. Monitorar el trànsit de xarxa d'una consulta DNS utilitzant una eina com ara el Wireshark.
4. Utilitzar eines de consulta DNS per aprendre el funcionament del protocol, com ara *dig*, *nslookup* i *host* (*host*). Examinar el procés que cal seguir a l'hora de fer una consulta.
5. Consultar la configuració del client DNS o resolutor.

b) Instal·lar i configurar un servidor DNS

1. Instal·lar un servidor DNS (per exemple, BIND). Observar quins components té: fitxers executables (especialment, el dimoni), fitxers de configuració, de documentació i de monitoratge.
2. Activar i desactivar el servei DNS. Establir els nivells d'arrencada en què s'ha d'executar el servei per defecte.
3. Monitorar les activitats que duu a terme el servidor per mitjà dels fitxers de registre (*logs*) del sistema. Identificar el nombre de procés (PID, *process identifier*) del servidor.
4. Observar els altres paràmetres de configuració que permet el servidor.
5. Monitorar el trànsit que genera el servidor DNS utilitzant el Wireshark.

a) Comprendre el funcionament general del protocol DNS

1. Fer la llista dels ports

En sistemes GNU/Linux, el fitxer `/etc/services` normalment conté la llista dels serveis associats a cada port. D'aquest fitxer es pot observar quins utilitza el protocol DNS.

Llista dels ports que inclouen alguna referència DNS:

```
[root@portatil ~]# cat /etc/services | grep DNS
[root@portatil ~]# cat /etc/services | grep dns
dnssix          90/tcp          # DNSIX Securit Attribute Token Map
dnssix          90/udp          # DNSIX Securit Attribute Token Map
sdnsskmp        558/tcp         # SDNSKMP
sdnsskmp        558/udp         # SDNSKMP
dns2go          1227/tcp        # DNS2Go
dns2go          1227/udp        # DNS2Go
menandmice-dns  1337/tcp        # menandmice DNS
menandmice-dns  1337/udp        # menandmice DNS
sunscalar-dns   1870/tcp        # SunSCALAR DNS Service
sunscalar-dns   1870/udp        # SunSCALAR DNS Service
ddns-v3         2164/tcp        # Dynamic DNS Version 3
ddns-v3         2164/udp        # Dynamic DNS Version 3
spw-dnspreload  3849/tcp        # SPACEWAY DNS Preload
spw-dnspreload  3849/udp        # SPACEWAY DNS Preload
dns-llq         5352/tcp        # DNS Long-Lived Queries
dns-llq         5352/udp        # DNS Long-Lived Queries
mdns            5353/tcp        # Multicast DNS
mdns            5353/udp        # Multicast DNS
```

De fet, però, sabem que el servei DNS utilitza el port 53 i no apareix en la llista. Si observem el fitxer `/etc/services`, veurem que s'indica amb el terme *domain* ('domini').

```
[root@portatil ~]# cat /etc/services | grep domain
domain          53/tcp          # name-domain
server
domain          53/udp
```

2. Monitorar el trànsit UDP del protocol DNS

Utilitat *iptraf*

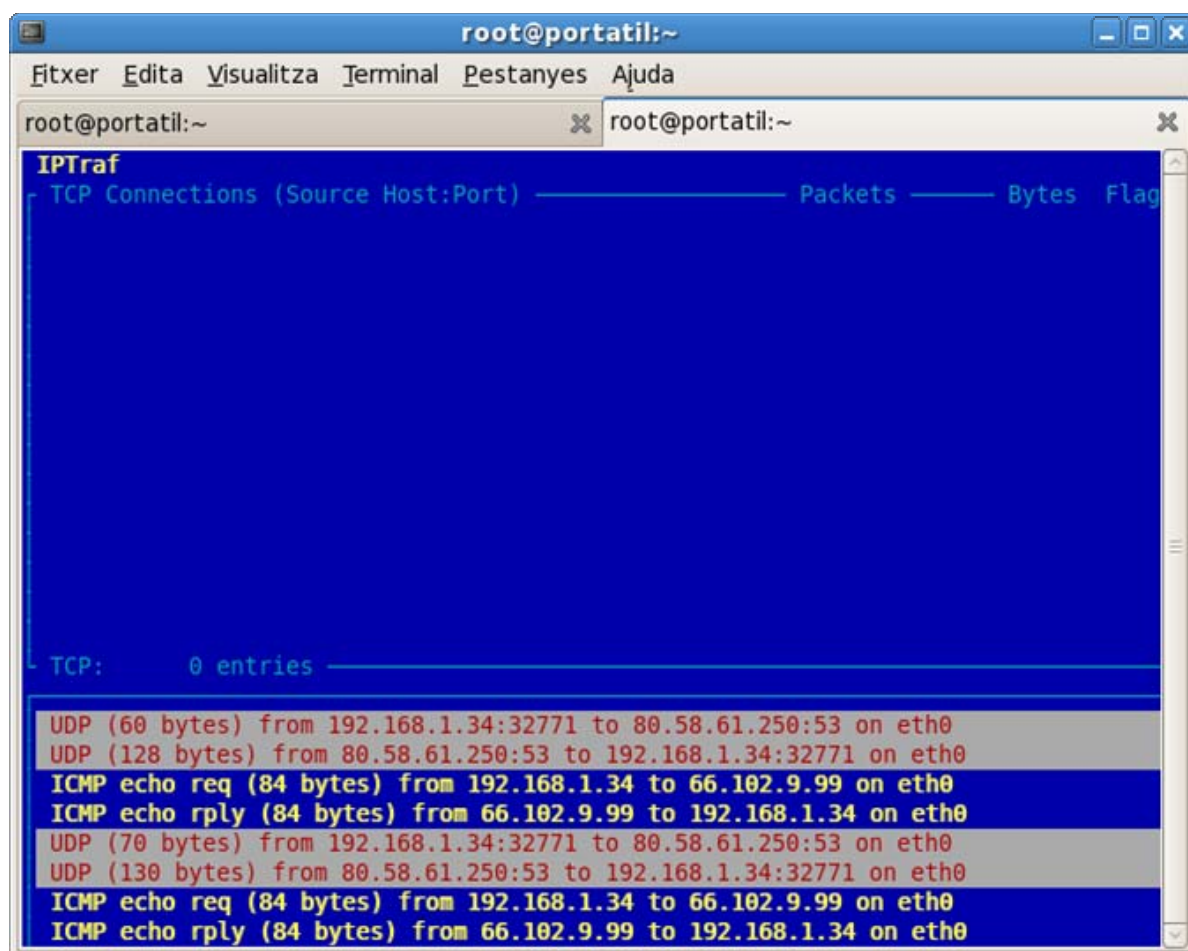
Podem observar el trànsit UDP d'una consulta DNS amb la utilitat *iptraf*, en què es pot veure la connexió del client de sortida utilitzant el port dinàmic 32771 en el port 53 del servidor 80.58.61.250. D'una banda activarem *iptraf*, i de l'altra, farem una consulta que requereixi resolució DNS.

```
[root@portatil ~]# ping www.google.com
```

```
PING www.l.google.com (66.102.9.99) 56(84) bytes of data.  
64 bytes from 66.102.9.99: icmp_seq=1 ttl=244 time=114 ms  
64 bytes from 66.102.9.99: icmp_seq=2 ttl=244 time=74.7 ms  
  
--- www.l.google.com ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 999ms  
rtt min/avg/max/mdev = 74.735/94.539/114.343/19.804 ms
```

En una altra sessió, prèviament hem fet el següent:

```
[root@portatil ~]# iptraf
```



Utilitat *nmap*

Podem fer la llista de l'estat del port en què escolta el servidor DNS:

```
[root@dnsServer ~]# nmap localhost  
Starting Nmap 4.20 ( http://insecure.org ) at 2008-06-07 14:50 CEST  
Interesting ports on localhost (127.0.0.1):  
Not shown: 1692 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
53/udp    open  dns  
80/tcp    open  http  
111/tcp   open  rpcbind
```

```
443/tcp open  https
8000/tcp open  http-alt
Nmap finished: 1 IP address (1 host up) scanned in 0.116 seconds
```

3 Monitorar el trànsit de xarxa amb el Wireshark

Podeu consultar l'exercici 5 de l'apartat *b* "Servidor DNS" d'aquest mateix annex, en què també es captura el trànsit DNS utilitzant el programa Wireshark.

4 Consultes amb *dig*, *nslookup* i *hoste*

Les utilitats *dig*, *nslookup* i *hoste* (*host*) permeten obtenir informació dels recursos d'un servidor DNS, resoldre consultes i saber quins registres de recurs contenen.

Utilitat *dig*

Tot seguit mostrem un exemple de consulta dels registres de recurs del servidor *fpoberta.net*:

```
[root@portatil ~]# dig fpoberta.net ANY

; <<>> DiG 9.4.2 <<>> fpoberta.net ANY
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9302
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;fpoberta.net.                IN      ANY

;; ANSWER SECTION:
fpoberta.net.                86275   IN      SOA     tibet.uoc.es. root.tibet.uoc.es.
2005121400 86400 7200 2592000 172800
fpoberta.net.                50451   IN      NS      tibet.uoc.es.
fpoberta.net.                50451   IN      NS      nepal.uoc.es.
fpoberta.net.                50451   IN      NS      bulgaria.uoc.es.
fpoberta.net.                50451   IN      MX      10 smtp.uoc.edu.

;; AUTHORITY SECTION:
fpoberta.net.                50451   IN      NS      bulgaria.uoc.es.
fpoberta.net.                50451   IN      NS      nepal.uoc.es.
fpoberta.net.                50451   IN      NS      tibet.uoc.es.

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Mon Dec 17 18:43:46 2007
;; MSG SIZE rcvd: 210
```

En l'exemple següent es consulten quins servidors tenen la denominació *root* ('arrel'):

```
[root@portatil ~]# dig . ANY
; <<>> DiG 9.4.2 <<>> . ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47921
;; flags: qr rd ra; QUERY: 1, ANSWER: 14, AUTHORITY: 13, ADDITIONAL: 3

;; QUESTION SECTION:
;.                               IN              ANY

;; ANSWER SECTION:
.                240358  IN          NS          H.ROOT-SERVERS.NET.
.                240358  IN          NS          B.ROOT-SERVERS.NET.
.                240358  IN          NS          I.ROOT-SERVERS.NET.
.                240358  IN          NS          K.ROOT-SERVERS.NET.
.                240358  IN          NS          J.ROOT-SERVERS.NET.
.                240358  IN          NS          C.ROOT-SERVERS.NET.
.                240358  IN          NS          G.ROOT-SERVERS.NET.
.                240358  IN          NS          L.ROOT-SERVERS.NET.
.                240358  IN          NS          E.ROOT-SERVERS.NET.
.                240358  IN          NS          M.ROOT-SERVERS.NET.
.                240358  IN          NS          F.ROOT-SERVERS.NET.
.                240358  IN          NS          D.ROOT-SERVERS.NET.
.                240358  IN          NS          A.ROOT-SERVERS.NET.
.                62937   IN          SOA         A.ROOT-SERVERS.NET. NSTLD.VERISIGN-
GRS.COM. 2007121601 1800 900 604800 86400

;; AUTHORITY SECTION:
.                240358  IN          NS          L.ROOT-SERVERS.NET.
.                240358  IN          NS          A.ROOT-SERVERS.NET.
.                240358  IN          NS          D.ROOT-SERVERS.NET.
.                240358  IN          NS          J.ROOT-SERVERS.NET.
.                240358  IN          NS          H.ROOT-SERVERS.NET.
.                240358  IN          NS          C.ROOT-SERVERS.NET.
.                240358  IN          NS          I.ROOT-SERVERS.NET.
.                240358  IN          NS          M.ROOT-SERVERS.NET.
.                240358  IN          NS          B.ROOT-SERVERS.NET.
.                240358  IN          NS          G.ROOT-SERVERS.NET.
.                240358  IN          NS          F.ROOT-SERVERS.NET.
.                240358  IN          NS          E.ROOT-SERVERS.NET.
.                240358  IN          NS          K.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET. 601520  IN          A           198.41.0.4
B.ROOT-SERVERS.NET. 581337  IN          A           192.228.79.201
C.ROOT-SERVERS.NET. 581337  IN          A           192.33.4.12

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Mon Dec 17 19:02:12 2007
;; MSG SIZE  rcvd: 502
```

L'exemple següent mostra la consulta dels servidors autoritaris que hi ha per al domini *.com*:

```

[root@portatil ~]# dig com. ANY
; <<>> DiG 9.4.2 <<>> com. ANY
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34936
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 13, ADDITIONAL: 3

;; QUESTION SECTION:
com.                IN      ANY

;; ANSWER SECTION:
com.                80008   IN      NS      h.gtld-servers.net.
com.                80008   IN      NS      k.gtld-servers.net.
com.                80008   IN      NS      b.gtld-servers.net.
com.                80008   IN      NS      i.gtld-servers.net.
com.                80008   IN      NS      m.gtld-servers.net.
com.                80008   IN      NS      l.gtld-servers.net.
com.                80008   IN      NS      e.gtld-servers.net.
com.                80008   IN      NS      j.gtld-servers.net.
com.                80008   IN      NS      f.gtld-servers.net.
com.                80008   IN      NS      a.gtld-servers.net.
com.                80008   IN      NS      g.gtld-servers.net.
com.                80008   IN      NS      c.gtld-servers.net.
com.                80008   IN      NS      d.gtld-servers.net.

;; AUTHORITY SECTION:
com.                80008   IN      NS      c.gtld-servers.net.
com.                80008   IN      NS      j.gtld-servers.net.
com.                80008   IN      NS      g.gtld-servers.net.
com.                80008   IN      NS      h.gtld-servers.net.
com.                80008   IN      NS      k.gtld-servers.net.
com.                80008   IN      NS      i.gtld-servers.net.
com.                80008   IN      NS      e.gtld-servers.net.
com.                80008   IN      NS      l.gtld-servers.net.
com.                80008   IN      NS      f.gtld-servers.net.
com.                80008   IN      NS      a.gtld-servers.net.
com.                80008   IN      NS      b.gtld-servers.net.
com.                80008   IN      NS      m.gtld-servers.net.
com.                80008   IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 72862   IN      A       192.5.6.30
a.gtld-servers.net. 79678   IN      AAAA    2001:503:a83e::2:30
b.gtld-servers.net. 72862   IN      A       192.33.14.30

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Mon Dec 17 19:02:50 2007
;; MSG SIZE rcvd: 487

```

Utilitat *nslookup*

Podem utilitzar la utilitat *nslookup* per fer consultes DNS de qualsevol tipus. Fins i tot es pot seleccionar el servidor al qual s'adrecen les consultes.

Observar quins nodes són *root*:

```
nslookup:
> .
Server:          192.168.0.10
Address:         192.168.0.10#53

Non-authoritative answer:
.       nameserver = G.ROOT-SERVERS.NET.
.       nameserver = F.ROOT-SERVERS.NET.
.       nameserver = L.ROOT-SERVERS.NET.
.       nameserver = I.ROOT-SERVERS.NET.
.       nameserver = E.ROOT-SERVERS.NET.
.       nameserver = K.ROOT-SERVERS.NET.
.       nameserver = A.ROOT-SERVERS.NET.
.       nameserver = C.ROOT-SERVERS.NET.
.       nameserver = M.ROOT-SERVERS.NET.
.       nameserver = H.ROOT-SERVERS.NET.
.       nameserver = D.ROOT-SERVERS.NET.
.       nameserver = J.ROOT-SERVERS.NET.
.       nameserver = B.ROOT-SERVERS.NET.
.
      origin = A.ROOT-SERVERS.NET
      mail addr = NSTLD.VERISIGN-GRS.COM
      serial = 2007121601
      refresh = 1800
      retry = 900
      expire = 604800
      minimum = 86400

Authoritative answers can be found from:
.       nameserver = J.ROOT-SERVERS.NET.
.       nameserver = F.ROOT-SERVERS.NET.
.       nameserver = K.ROOT-SERVERS.NET.
.       nameserver = I.ROOT-SERVERS.NET.
.       nameserver = C.ROOT-SERVERS.NET.
.       nameserver = D.ROOT-SERVERS.NET.
.       nameserver = M.ROOT-SERVERS.NET.
.       nameserver = G.ROOT-SERVERS.NET.
.       nameserver = E.ROOT-SERVERS.NET.
.       nameserver = A.ROOT-SERVERS.NET.
.       nameserver = B.ROOT-SERVERS.NET.
.       nameserver = L.ROOT-SERVERS.NET.
.       nameserver = H.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET      internet address = 198.41.0.4
B.ROOT-SERVERS.NET      internet address = 192.228.79.201
C.ROOT-SERVERS.NET      internet address = 192.33.4.12
```

Observar els noms dels servidors autoritaris per al domini *.cat*:

```
nslookup:
> cat
Server:          192.168.0.10
Address:         192.168.0.10#53

Non-authoritative answer:
cat
```

```
origin = ns.nic.cat
mail addr = dnsmaster.knipp.de
serial = 2007121773
refresh = 10800
retry = 10800
expire = 604800
minimum = 86400
cat      nameserver = ns1.nic.es.
cat      nameserver = merapi.switch.ch.
cat      nameserver = ns-ext.nrt1.isc.org.
cat      nameserver = ns.nic.cat.
cat      nameserver = ns-ext.isc.org.
cat      nameserver = ns5.knipp.de.
cat      nameserver = dns4.ad.
cat      nameserver = cat-dns.denic.de.
cat      nameserver = dns-cat.pch.net.
```

Authoritative answers can be found from:

```
cat      nameserver = dns4.ad.
cat      nameserver = ns1.nic.es.
cat      nameserver = ns-ext.nrt1.isc.org.
cat      nameserver = ns-ext.isc.org.
cat      nameserver = merapi.switch.ch.
cat      nameserver = cat-dns.denic.de.
cat      nameserver = dns-cat.pch.net.
cat      nameserver = ns.nic.cat.
cat      nameserver = ns5.knipp.de.
ns1.nic.es      internet address = 194.69.254.1
ns5.knipp.de    internet address = 195.253.6.62
dns4.ad internet address = 194.158.64.10
ns-ext.isc.org  internet address = 204.152.184.64
```

Si utilitzem el servidor de noms d'un altre domini, per exemple *dns.gencat.net*, també podem fer-hi consultes:

nslookup

```
> server 83.247.128.1
```

```
Default server: 83.247.128.1
```

```
Address: 83.247.128.1#53
```

```
> set type=any
```

```
> mail.yahoo.com
```

```
Server:      83.247.128.1
```

```
Address:     83.247.128.1#53
```

Non-authoritative answer:

```
mail.yahoo.com canonical name = login.yahoo.com.
```

Authoritative answers can be found from:

```
yahoo.com      nameserver = ns2.yahoo.com.
yahoo.com      nameserver = ns1.yahoo.com.
yahoo.com      nameserver = ns3.yahoo.com.
yahoo.com      nameserver = ns4.yahoo.com.
yahoo.com      nameserver = ns5.yahoo.com.
yahoo.com      nameserver = ns6.yahoo.com.
yahoo.com      nameserver = ns8.yahoo.com.
ns2.yahoo.com   internet address = 68.142.255.16
ns1.yahoo.com   internet address = 66.218.71.63
ns3.yahoo.com   internet address = 217.12.4.104
```

ns4.yahoo.com	internet address = 68.142.196.63
ns5.yahoo.com	internet address = 216.109.116.17
ns6.yahoo.com	internet address = 202.43.223.170
ns8.yahoo.com	internet address = 202.165.104.22

Utilitat hoste

Per saber a qui correspon l'adreça IP utilitzada en l'exemple anterior:

```
[root@portatil ~]# host 83.247.128.1
1.128.247.83.in-addr.arpa domain name pointer dns.gencat.net.
```

Per veure la informació del domini de la UOC:

```
[root@portatil ~]# host -a uoc.es
Trying "uoc.es"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51683
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;uoc.es.                IN      ANY

;; ANSWER SECTION:
uoc.es.                 86400   IN      NS      nepal.uoc.es.
uoc.es.                 86400   IN      NS      tibet.uoc.es.
uoc.es.                 86400   IN      SOA     tibet.uoc.es. root.tibet.uoc.es.
2008062000 28800 7200 604800 86400

;; ADDITIONAL SECTION:
nepal.uoc.es.           86077   IN      A       213.73.40.47
tibet.uoc.es.           86077   IN      A       213.73.40.45

Received 137 bytes from 80.58.61.250#53 in 97 ms
```

Per veure els servidors de correu de Google:

```
[root@portatil ~]# host -t MX google.com
google.com mail is handled by 10 smtp1.google.com.
google.com mail is handled by 10 smtp2.google.com.
google.com mail is handled by 10 smtp3.google.com.
google.com mail is handled by 10 smtp4.google.com.
```

5. Consultar la configuració del client: sistema de resolució

El client d'una consulta DNS utilitza el sistema de resolució (*resolver*). Es tracta de biblioteques amb les quals està enllaçada l'aplicació client corresponent. És a dir, no hi ha un programa de resolució client, sinó que el Firefox n'implementa un, el sistema de xarxa un altre, etc.

El fitxer que conté la configuració del sistema de resolució en sistemes GNU/Linux és el */etc/resolv.conf*.

```
[root@portatil ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search escola.org
nameserver 80.58.61.250
nameserver 80.58.61.254
```

L'ordre en què s'han de resoldre les consultes client pot ser el següent: de primer, mirar els fitxers de configuració local (normalment, el fitxer */etc/hosts*) i, després, consultar un servidor DNS, o a l'inrevés. Aquesta configuració es defineix en el fitxer */etc/nsswitch*.

```
[root@portatil ~]# cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#      nisplus or nis+      Use NIS+ (NIS version 3)
#      nis or yp            Use NIS (NIS version 2), also called YP
#      dns                  Use DNS (Domain Name Service)
#      files                Use the local files
#      db                   Use the local database (.db) files
#      compat               Use NIS on compat mode
#      hesiod               Use Hesiod for user lookups
#      [NOTFOUND=return]    Stop searching if not found so far
#
# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis
#
passwd:     files
shadow:     files
group:      files
#
#hosts:     db files nisplus nis dns
hosts:      files dns
```

b) Instal·lar i configurar un servidor DNS

1. Instal·lar el servidor DNS i observar-ne els components

Instal·lar el programari servidor

Buscar per Internet paquets del client i del servidor DNS a Google, en repositoris de programari, etc. Si es disposa de *yum* o de *apt-get* o *wget*:

Llista de paquets *rpm* que contenen el text *bind*:

```
[root@portatil ~]# yum list bind
Installed Packages
bind.i386                               31:9.4.2-3.fc7
installed
Available Packages
bind.i386                               31:9.4.2-4.fc7
updates
```

Llista de paquets que contenen *bind**:

```
[root@portatil ~]# yum list bind*
Installed Packages
bind.i386                               31:9.4.2-3.fc7      installed
bind-libs.i386                         31:9.4.2-3.fc7      installed
bind-utils.i386                       31:9.4.2-3.fc7      installed
Available Packages
bind.i386                               31:9.4.2-4.fc7      updates
bind-chroot.i386                      31:9.4.2-4.fc7      updates
bind-devel.i386                       31:9.4.2-4.fc7      updates
bind-libs.i386                        31:9.4.2-4.fc7      updates
bind-sdb.i386                         31:9.4.2-4.fc7      updates
bind-utils.i386                      31:9.4.2-4.fc7      updates
```

Instal·lar el paquet *bind*:

```
# yum install bind
```

Fer la llista dels paquets *bind* instal·lats. Si el sistema ja els té instal·lats, o ho volem comprovar, podem consultar els paquets instal·lats:

```
[root@portatil ~]# rpm -qa | grep bind
ypbind-1.19-9.fc7
system-config-bind-4.0.2-6.fc7
rpcbind-0.1.4-8.fc7
bind-libs-9.4.2-3.fc7
bind-9.4.2-3.fc7
bind-utils-9.4.2-3.fc7
```

Obtenir informació del paquet del servei *bind*:

```
[root@portatil ~]# rpm -qi bind
```

```
Name       : bind                               Relocations: (not relocatable)
Version    : 9.4.2                             Vendor: Fedora Project
Release    : 3.fc7                             Build Date: dl 21 gen 2008 11:27:32 CET
Install Date: dc 23 gen 2008 19:12:18 CET       Build Host:
xenbuilder4.fedora.phx.redhat.com
Group      : System Environment/Daemons        Source RPM: bind-9.4.2-3.fc7.src.rpm
Size       : 3627903                           License: BSD-like
Signature  : DSA/SHA1, dl 21 gen 2008 19:48:26 CET, Key ID b44269d04f2a6fd2
Packager   : Fedora Project
URL        : http://www.isc.org/products/BIND/
Summary    : El servidor de noms de domini (DNS) Berkley Internet Name Domain (BIND).
Description:
El BIND (Berkeley Internet Name Domain) és una implementació de protocol
DNS (sistema de noms de domini). El BIND inclou un servidor DNS (named),
que converteix els noms d'ordinador en adreces IP, una biblioteca per
a resoldre els noms (rutines per aplicacions que usen DNS), i eines per
a verificar que el servidor DNS funciona degudament.
```

Observar els components del paquet

Fer la llista dels components del paquet *bind*:

```
[root@portatil ~]# rpm -ql bind
```

```
/etc/dbus-1/system.d/named.conf
/etc/logrotate.d/named
/etc/named.conf
/etc/rc.d/init.d/named
/etc/rndc.conf
/etc/rndc.key
/etc/sysconfig/named
/usr/sbin/dns-keygen
/usr/sbin/dnssec-keygen
/usr/sbin/dnssec-signzone
/usr/sbin/lwresd
/usr/sbin/named
/usr/sbin/named-bootconf
/usr/sbin/named-checkconf
/usr/sbin/named-checkzone
/usr/sbin/named-compilezone
/usr/sbin/namedGetForwarders
/usr/sbin/namedSetForwarders
/usr/sbin/rndc
/usr/sbin/rndc-confgen
/usr/share/dbus-1/services/named.service
... output suprimir ...
/usr/share/doc/bind-
9.4.2/sample/var/named/slaves/my.slave.internal.zone.db
/usr/share/man/man5/named.conf.5.gz
... output suprimir ...
/usr/share/man/man8/rndc.8.gz
/var/named
/var/named/data
/var/named/dynamic
/var/named/slaves
/var/run/named
```

Segons el directori on s'ubiquen podem intuir si són executables, de configuració o de documentació. També podem intentar filtrar la sortida en cada cas.

Fitxers de configuració:

```
[root@portatil ~]# rpm -qc bind
/etc/dbus-1/system.d/named.conf
/etc/logrotate.d/named
/etc/named.conf
/etc/rc.d/init.d/named
/etc/rndc.conf
/etc/rndc.key
/etc/sysconfig/named
/usr/share/dbus-1/services/named.service
```

```
[root@portatil ~]# rpm -ql bind | grep etc
/etc/dbus-1/system.d/named.conf
/etc/logrotate.d/named
/etc/named.conf
/etc/rc.d/init.d/named
/etc/rndc.conf
/etc/rndc.key
/etc/sysconfig/named
/usr/share/doc/bind-9.4.2/sample/etc
/usr/share/doc/bind-9.4.2/sample/etc/named.conf
/usr/share/doc/bind-9.4.2/sample/etc/rndc.conf
```

Fitxers de documentació:

```
[root@portatil ~]# rpm -qd bind
/usr/share/doc/bind-9.4.2/CHANGES
/usr/share/doc/bind-9.4.2/COPYRIGHT
/usr/share/doc/bind-9.4.2/README
/usr/share/doc/bind-9.4.2/README.DBUS
/usr/share/doc/bind-9.4.2/arm/Bv9ARM-book.xml
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch01.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch02.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch03.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch04.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch05.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch06.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch07.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch08.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch09.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.ch10.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.html
/usr/share/doc/bind-9.4.2/arm/Bv9ARM.pdf
/usr/share/doc/bind-9.4.2/arm/Makefile
/usr/share/doc/bind-9.4.2/arm/Makefile.in
/usr/share/doc/bind-9.4.2/arm/README-SGML
/usr/share/doc/bind-9.4.2/arm/isc-logo.eps
/usr/share/doc/bind-9.4.2/arm/isc-logo.pdf
/usr/share/doc/bind-9.4.2/arm/latex-fixup.pl
/usr/share/doc/bind-9.4.2/arm/man.dig.html
/usr/share/doc/bind-9.4.2/arm/man.dnssec-keygen.html
```

```
/usr/share/doc/bind-9.4.2/arm/man.dnssec-signzone.html
/usr/share/doc/bind-9.4.2/arm/man.host.html
/usr/share/doc/bind-9.4.2/arm/man.named-checkconf.html
/usr/share/doc/bind-9.4.2/arm/man.named-checkzone.html
/usr/share/doc/bind-9.4.2/arm/man.named.html
/usr/share/doc/bind-9.4.2/arm/man.rndc-confgen.html
/usr/share/doc/bind-9.4.2/arm/man.rndc.conf.html
/usr/share/doc/bind-9.4.2/arm/man.rndc.html
/usr/share/doc/bind-9.4.2/misc/Makefile
/usr/share/doc/bind-9.4.2/misc/Makefile.in
/usr/share/doc/bind-9.4.2/misc/dnssec
/usr/share/doc/bind-9.4.2/misc/format-options.pl
/usr/share/doc/bind-9.4.2/misc/ipv6
/usr/share/doc/bind-9.4.2/misc/migration
/usr/share/doc/bind-9.4.2/misc/migration-4to9
/usr/share/doc/bind-9.4.2/misc/options
/usr/share/doc/bind-9.4.2/misc/options.edns
/usr/share/doc/bind-9.4.2/misc/rfc-compliance
/usr/share/doc/bind-9.4.2/misc/roadmap
/usr/share/doc/bind-9.4.2/misc/sdb
/usr/share/doc/bind-9.4.2/sample/etc/named.conf
/usr/share/doc/bind-9.4.2/sample/etc/rndc.conf
/usr/share/doc/bind-9.4.2/sample/named.ca
/usr/share/doc/bind-9.4.2/sample/named.empty
/usr/share/doc/bind-9.4.2/sample/named.localhost
/usr/share/doc/bind-9.4.2/sample/named.loopback
/usr/share/doc/bind-9.4.2/sample/named.rfc1912.zones
/usr/share/doc/bind-9.4.2/sample/var/named/my.external.zone.db
/usr/share/doc/bind-9.4.2/sample/var/named/my.internal.zone.db
/usr/share/doc/bind-9.4.2/sample/var/named/slaves/my.ddns.internal.zone.db
/usr/share/doc/bind-9.4.2/sample/var/named/slaves/my.slave.internal.zone.db
/usr/share/man/man5/named.conf.5.gz
/usr/share/man/man5/rndc.conf.5.gz
/usr/share/man/man8/dnssec-keygen.8.gz
/usr/share/man/man8/dnssec-signzone.8.gz
/usr/share/man/man8/lwresd.8.gz
/usr/share/man/man8/named-checkconf.8.gz
/usr/share/man/man8/named-checkzone.8.gz
/usr/share/man/man8/named-compilezone.8.gz
/usr/share/man/man8/named.8.gz
/usr/share/man/man8/rndc-confgen.8.gz
/usr/share/man/man8/rndc.8.gz
```

Podem intentar filtrar quins són els executables, tenint en compte que normalment seran en un directori anomenat *bin* o *sbin*.

```
[root@portatil ~]# rpm -ql bind | grep bin/
/usr/sbin/dns-keygen
/usr/sbin/dnssec-keygen
/usr/sbin/dnssec-signzone
/usr/sbin/lwresd
/usr/sbin/named
/usr/sbin/named-bootconf
/usr/sbin/named-checkconf
/usr/sbin/named-checkzone
/usr/sbin/named-compilezone
/usr/sbin/namedGetForwarders
/usr/sbin/namedSetForwarders
```

```
/usr/sbin/rndc
/usr/sbin/rndc-confgen
```

Resum

- Els fitxers de documentació normalment són a `/usr/share/doc` i a `/usr/share/man`.
- Els fitxers de configuració són a `/etc`, `/etc/sysconfig`.
- El dimoni del servei és a `/usr/sbin/named`.
- El fitxer de configuració del dimoni del servei és `/etc/named.conf`.
- El fitxer de govern del servei és `/etc/rc.d/init.d/named`.
- El fitxer de configuració dels fitxers de registre és a `/etc/logrotate.d/named`.

2. Activar o desactivar el servei i establir els nivells d'arrencada

El servei

Primerament cal saber si el servidor instal·lat funciona de manera autònoma (*stand-alone*) o dins del superdimoni de xarxa *xinetd* o *initd*. Si hi ha fitxers de configuració dins del directori `/etc/xinetd.d/<nom-servei>`, es tracta d'un servei dins del *xinetd*. Si hi ha fitxers de configuració dins del directori `/etc/rc.d/init.d/<nom-servei>`, es tracta d'un servei autònom.

Observem el contingut del paquet per esbrinar si els fitxers de configuració ens permeten saber de quin tipus de servei es tracta:

```
[root@portatil ~]# rpm -ql bind | grep /etc
/etc/dbus-1/system.d/named.conf
/etc/logrotate.d/named
/etc/named.conf
/etc/rc.d/init.d/named
/etc/rndc.conf
/etc/rndc.key
/etc/sysconfig/named
/usr/share/doc/bind-9.4.2/sample/etc
/usr/share/doc/bind-9.4.2/sample/etc/named.conf
/usr/share/doc/bind-9.4.2/sample/etc/rndc.conf
```

Com podem veure, es tracta d'un servei autònom. També es pot consultar el tipus de servei amb l'ordre **chkconfig** i observar si surt en la llista d'una manera o de l'altra:

```
[root@portatil ~]# chkconfig --list | grep named
named          0:apagat      1:apagat      2:apagat
3:apagat       4:apagat      5:apagat      6:apagat
```

Per facilitar la cerca dels serveis autònoms podem fer el següent:

```
[root@portatil ~]# chkconfig --list named
named          0:apagat      1:apagat      2:apagat
3:apagat       4:apagat      5:apagat      6:apagat
```

Estat del servei

Podem saber l'estat del servei amb l'opció estat (*status*) de les ordres:

```
[root@portatil ~]# service named status
named      està aturat
[root@portatil ~]# /etc/rc.d/init.d/named status
named      està aturat
```

Podem arrencar el servei amb l'opció engegada (*start*) de les ordres:

```
[root@portatil ~]# service named start
S'està iniciant el servei named:          [ FET  ]
[root@portatil ~]# /etc/rc.d/init.d/named start
S'està iniciant el servei named:          [ FET  ]
```

Podem parar el servei amb l'opció aturada (*stop*) de les ordres:

```
[root@portatil ~]# service named stop
S'està aturant el named:                  [ FET  ]
[root@portatil ~]# /etc/rc.d/init.d/named stop
S'està aturant el servei named:           [ FET  ]
```

Podem tornar a iniciar el servei amb l'opció recarregar (*reload*) o reiniciar (*restart*) de les ordres:

```
[root@portatil ~]# /etc/rc.d/init.d/named restart
S'està aturant el servei named:
[Incorrecte]
S'està iniciant el servei named:          [ FET  ]
[root@portatil ~]# service named reload
S'està aturant el servei named:          [ FET  ]
S'està iniciant el servei named:          [ FET  ]
```

Per saber les ordres possibles:

```
[root@portatil ~]# service named patapum
Forma d'ús: /etc/init.d/dhcpd {start|stop|restart|condrestart|status}
[root@portatil ~]# /etc/rc.d/init.d/named pimpam
Forma d'ús: /etc/rc.d/init.d/dhcpd {start|stop|restart|condrestart|status}
```

Establir els nivells del servei per defecte

Els serveis (els dimonis executables) es poden configurar per arrencar automàticament en determinats nivells d'execució. Les màquines

GNU/Linux tenen set nivells d'execució, tal com es pot veure en el fitxer `/etc/inittab`.

```
[root@portatil ~]# head -20 /etc/inittab
... output suprimir ...
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
# ... output suprimir ...
```

Per configurar els nivells als quals es vol que s'executi un servei s'utilitza l'ordre **chkconfig**, que permet activar o desactivar el servei per als nivells indicats.

```
[root@portatil ~]# chkconfig --list dhcpd
dhcpd          0:apagat    1:apagat    2:apagat
3:apagat       4:apagat    5:apagat    6:apagat
```

```
[root@portatil ~]# chkconfig --help
chkconfig versió 1.3.34 - Copyright (C) 1997-2000 Red Hat, Inc.
Aquest programari es pot distribuir lliurement d'acord amb els termes de la Llicència Pública General GNU.
forma d'ús:  chkconfig --list [nom]
            chkconfig --add <nom>
            chkconfig --del <nom>
            chkconfig --override <nom>
            chkconfig [--level <nivells>] <nom> <on|off|reset|resetpriorities>
```

```
[root@portatil ~]# chkconfig --level 345 namedd on
[root@portatil ~]# chkconfig --list | grep named
named          0:apagat    1:apagat    2:apagat
3:engagat      4:engagat    5:engagat    6:apagat
```

Fixeu-vos que definir els nivells d'execució no significa que el servei ara estigui engegat. Significa que quan arrenqui el sistema (a partir d'aquest moment) s'engegarà en els nivells corresponents. Podem ser en el nivell cinc i tenir el servei aturat perquè encara no l'hem engegat. Per exemple:

```
[root@portatil ~]# runlevel
N 5
[root@portatil ~]# service named status
named està aturat
[root@portatil ~]# service named start
S'està iniciant el servei named [ FET ]
```

3. Monitorar les activitats del servidor i del procés

Els fitxers de registre

El sistema enregistra les accions relacionades amb el servidor DNS en el fitxer de monitoratge estàndard `/var/log/messages`:

```
[root@portatil ~]# cat /var/log/messages | grep named
Jun 30 18:27:44 portatil named: zone localdomain/IN: loading from master file
localdomain.zone failed: file not found
Jun 30 18:27:44 portatil named: _default/localdomain/IN: file not found
Jun 30 18:27:44 portatil named: zone localhost/IN: loading from master file
localhost.zone failed: file not found
```

El procés del servei

Qualsevol procés en el sistema té un identificador de procés (PID, *process identifier*). Els PID dels serveis normalment es desen al sistema de fitxers (a `/var/run`) amb un valor numèric (en text) corresponent al PID.

Amb el servei en marxa sempre es pot observar el PID del servidor per mitjà de:

```
[root@portatil ~]# ps ax | grep named
3612 ?        Ss          0:00 /usr/sbin/named

[root@portatil ~]# service named status
named (pid 3612) s'està executant...

[root@portatil ~]# ll /var/run/named.pid
-rw-r--r-- 1 root root 5 29 jun 14:17 /var/run/named.pid
[root@portatil ~]# cat /var/run/named.pid
3612
```

La concurrència

Un cop iniciat el servei es crea un fitxer de bloqueig (*lock*) amb el nom del servei per evitar iniciar una altra instància. Els fitxers de bloqueig normalment es troben a `/var/lock` i són un simple fitxer de text buit en què el fet que hi siguin ja indica que el servei està en procés. En parar el servei el fitxer s'elimina.

Podem observar aquests fitxers amb el servei engegat:

```
[root@portatil ~]# cat /var/lock/subsys/named
[root@portatil ~]# ll /var/lock/subsys/named
-rw-r--r-- 1 root root 0 1 jun 18:26 /var/lock/subsys/named
```

4. Configuració del servei DNS

Configuració bàsica

Per fer funcionar el servidor DNS cal configurar-lo prèviament, ja que ha de saber quin domini administrarà i quins noms de màquina pertanyen al domini (definir els registres de recurs que cal utilitzar), entre molts altres paràmetres de configuració.

El paquet *dns* conté un fitxer d'exemple de configuració d'una zona en el directori `/usr/share/doc/bind-*/sample/etc/named.conf`. Aquest fitxer es pot copiar a `/etc/named.conf` i esdevindrà la configuració bàsica del servidor DNS.

```
[root@portatil ~]# rpm -ql bind | grep named.conf
/etc/dbus-1/system.d/named.conf
/etc/named.conf
/usr/share/doc/bind-9.4.2/sample/etc/named.conf
/usr/share/man/man5/named.conf.5.gz
```

Podeu fer la llista del contingut fent el següent:

```
[root@portatil ~]# ll /usr/share/doc/bind-9.4.2/sample/etc/named.conf
-rw-r--r-- 1 root root 4273 14 jun 2006 /usr/share/doc/bind-
9.4.2/sample/etc/named.conf
```

Observem-ne el contingut:

```
[root@portatil ~]# cat /usr/share/doc/bind-9.4.2/sample/etc/named.conf
//
// Sample named.conf BIND DNS server 'named' configuration file
// for the Red Hat BIND distribution.
//
// See the BIND Administrator's Reference Manual (ARM) for details, in:
//   file:///usr/share/doc/bind-*/arm/Bv9ARM.html
// Also see the BIND Configuration GUI : /usr/bin/system-config-bind and
// its manual.
//
options
{
    /* make named use port 53 for the source of all queries, to allow
     * firewalls to block all ports except 53:
     */
    query-source      port 53;
    query-source-v6   port 53;

    // Put files that named is allowed to write in the data/ directory:
    directory "/var/named"; // the default
    dump-file      "data/cache_dump.db";
    statistics-file "data/named_stats.txt";
    memstatistics-file "data/named_mem_stats.txt";
```

```
};
logging
{
/*      If you want to enable debugging, eg. using the 'rndc trace' command,
 *      named will try to write the 'named.run' file in the $directory (/var/named).
 *      By default, SELinux policy does not allow named to modify the /var/named
directory,
 *      so put the default debug log file in data/ :
 */
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};
//
// All BIND 9 zones are in a "view", which allow different zones to be served
// to different types of client addresses, and for options to be set for groups
// of zones.
//
// By default, if named.conf contains no "view" clauses, all zones are in the
// "default" view, which matches all clients.
//
// If named.conf contains any "view" clause, then all zones MUST be in a view;
// so it is recommended to start off using views to avoid having to restructure
// your configuration files in the future.
//
view "localhost_resolver"
{
/* This view sets up named to be a localhost resolver ( caching only nameserver ).
 * If all you want is a caching-only nameserver, then you need only define this view:
 */
    match-clients          { localhost; };
    match-destinations     { localhost; };
    recursion yes;
    # all views must contain the root hints zone:
    include "/etc/named.root.hints";

    /* these are zones that contain definitions for all the localhost
     * names and addresses, as recommended in RFC1912 - these names should
     * ONLY be served to localhost clients:
     */
    include "/etc/named.rfc1912.zones";
};
view "internal"
{
/* This view will contain zones you want to serve only to "internal" clients
   that connect via your directly attached LAN interfaces - "localnets" .
 */
    match-clients          { localnets; };
    match-destinations     { localnets; };
    recursion yes;
    // all views must contain the root hints zone:
    include "/etc/named.root.hints";

    // include "named.rfc1912.zones";
    // you should not serve your rfc1912 names to non-localhost clients.

    // These are your "authoritative" internal zones, and would probably
    // also be included in the "localhost_resolver" view above :

```

```

zone "my.internal.zone" {
    type master;
    file "my.internal.zone.db";
};
zone "my.slave.internal.zone" {
    type slave;
    file "slaves/my.slave.internal.zone.db";
    masters { /* put master nameserver IPs here */ 127.0.0.1; } ;
    // put slave zones in the slaves/ directory so named can update them
};
zone "my.ddns.internal.zone" {
    type master;
    allow-update { key ddns_key; };
    file "slaves/my.ddns.internal.zone.db";
    // put dynamically updateable zones in the slaves/ directory so named
can update them
};
};
key ddns_key
{
    algorithm hmac-md5;
    secret "use /usr/sbin/dns-keygen to generate TSIG keys";
};
view "external"
{
/* This view will contain zones you want to serve only to "external" clients
 * that have addresses that are not on your directly attached LAN interface subnets:
 */
    match-clients          { !localnets; !localhost; };
    match-destinations      { !localnets; !localhost; };

    recursion no;
    // you'd probably want to deny recursion to external clients, so you don't
    // end up providing free DNS service to all takers

    // all views must contain the root hints zone:
    include "/etc/named.root.hints";

    // These are your "authoritative" external zones, and would probably
    // contain entries for just your web and mail servers:

    zone "my.external.zone" {
        type master;
        file "my.external.zone.db";
    };
};
};

```

En la configuració per defecte es poden analitzar els diversos elements que es configuren:

- **options:** s'hi defineixen les opcions genèriques del servidor DNS.
- **loggin:** s'hi defineix el procés d'enregistrament dels fitxers de registre del servei.
- **localhost_resolver:** secció que permet definir el servidor DNS com a un servidor només cau. És a dir, no posseeix cap domini, no gestiona

cap domini ni zona i no té fitxers de zona. Únicament fa la funció de servidor DNS cau.

- **internal:** secció que permet definir les zones i zones delegades que es vol gestionar amb el servidor. Es donarà servei a les xarxes locals internes que es defineixen en aquesta secció.
- **external:** defineix el servei que cal oferir a clients externs a la xarxa local. És per oferir serveis DNS a clients exteriors.

Exemple de configuració bàsica

Com hem pogut observar, el fitxer d'exemple que proporciona *bind* és força complex. Una configuració per donar servei, per exemple a una escola, pot ser la següent.

Fitxer de configuració del servei *named* que es troba a */etc/named.conf*:

```
// named.conf for inf.escola.org
// vim:nowrap:

options {
    // definició d'opcions globals
    directory "/var/named";

    // query-source port 53;
    forward only;
    forwarders {
        100.1.1.201;
        100.1.1.202;
    };
};

//zone "." {
    // type hint;
    // file "root.hints";
//};

//zone "0.0.127.in-addr.arpa" {
    // definició del localhost
    // type master;
    // file "localhost.rev.zone";
//};

zone "inf.escola.org" {
    // definició per a la resolució directa
    notify no;
    type master;
    file "inf.escola.org.zone";
};

zone "0.16.172.in-addr.arpa" {
    // definició per a la resolució inversa
    notify no;
    type master;
    file "inf.escola.org.rev.zone";
};
```

El fitxer de zona per a la resolució directa esmentat en l'exemple anterior, *inf.escola.org.zone*, conté els registres de recurs que defineixen la zona.

```
; Zone file for inf.escola.org
$TTL 3D
@ IN SOA server.inf.escola.org. postmaster.inf.escola.org. (
                                2007101910 ; Serial
                                8H      ; Refresh
                                2H      ; Retry
                                4W      ; Expire
                                1D)    ; Minimum TTL

    NS      server
    MX      10 mailhost
    A       172.16.0.10

; loopback
localhost  A       127.0.0.1

; Ordinadors del departament
; subxarxa 172.16.0.0 mask 255.255.255.192
server     A 172.16.0.10
mailhost   A 172.16.0.10
www        CNAME  server
ftp        CNAME  server
ldap       CNAME  server

; Servidors, router, i impressora
router     A 172.16.0.1
hp-7200c   A 172.16.0.5

; Estacions departament. Adreça IP fixa i automàtica des de DHCP.
pcprofe01  A 172.16.0.15
pcprofe02  A 172.16.0.16

; Estacions aula-1. Adreça IP fixa i automàtica des de DHCP.
; subxarxa 172.16.0.128 mask 255.255.255.192
switch-A   A 172.16.0.251
pc01       A 172.16.0.131
pc02       A 172.16.0.132
```

Per a cada xarxa client que es defineix, cal definir el fitxer de resolució inversa de la xarxa en el domini *in-addr.arpa*. El fitxer de resolució inversa correspon a la denominació *inf.escola.org.rev.zone*. Aquí hi ha una entrada PTR per a cada hoste definit en la resolució directa.

```
; Zone file for 0.168.192.in-addr.arpa
$TTL 3D
@ IN SOA server.inf.escola.org. postmaster.inf.escola.org. (
                                2007101910 ; Serial
                                8H      ; Refresh
                                2H      ; Retry
                                4W      ; Expire
                                1D)    ; Minimum TTL

    NS      server.inf.escola.org.
; departament
```

```
1 PTR router.inf.escola.org.
5 PTR hp-7200c.inf.escola.org.
10PTR server.inf.escola.org.
15PTR pcprofe01.inf.escola.org.
16PTR pcprofe02.inf.escola.org.
131 PTR pc01.inf.escola.org.
132 PTR pc02.inf.escola.org.
251 PTR switch-A.inf.escola.org.
```

5. Monitorar el trànsit amb el Wireshark

Monitoratge

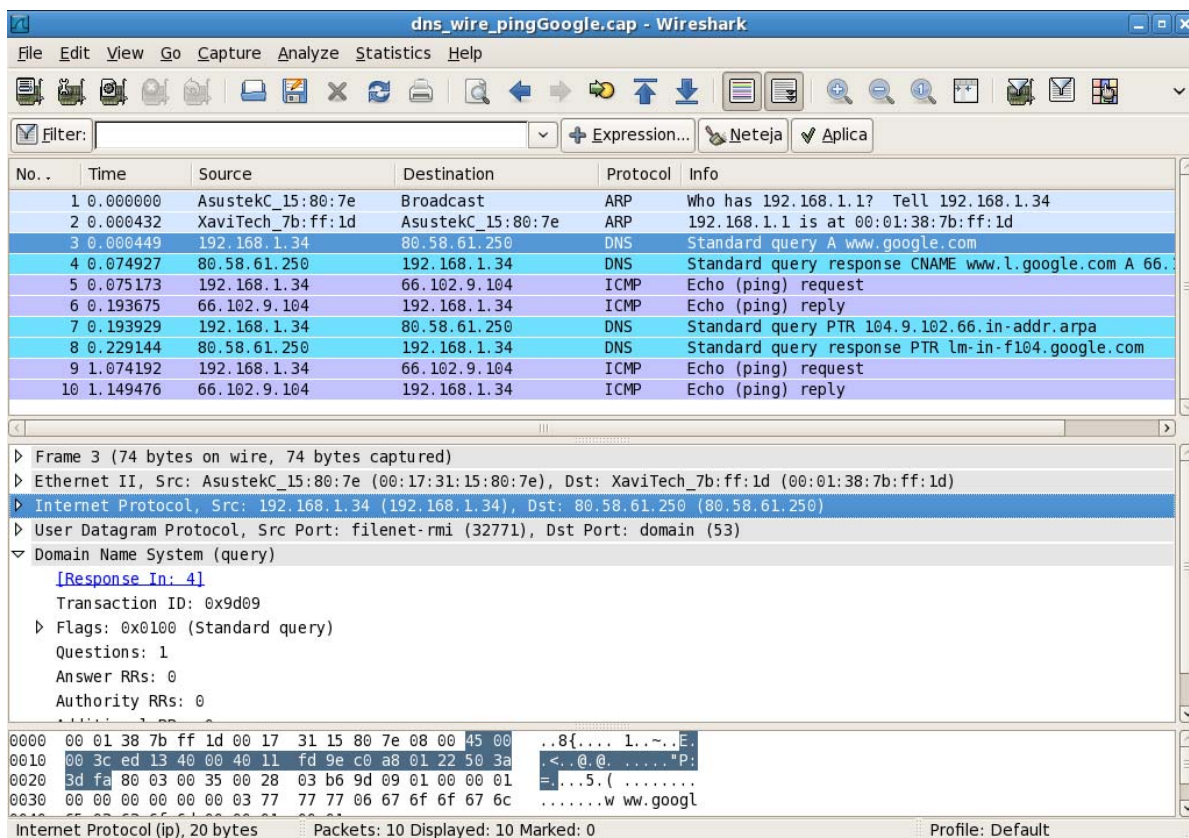
Activar un detector de xarxa, com per exemple el Wireshark, per monitorar el trànsit DNS.

Podem fer que el client sol·liciti una consulta DNS simplement fent un *ping* a una nova adreça IP que no estigui al servidor cau local i que calgui resoldre per mitjà de DNS.

```
[root@portatil ~]# ping www.google.com
PING www.l.google.com (66.102.9.104) 56(84) bytes of data.
64 bytes from lm-in-f104.google.com (66.102.9.104): icmp_seq=1 ttl=244 time=118 ms
64 bytes from lm-in-f104.google.com (66.102.9.104): icmp_seq=2 ttl=244 time=75.3 ms
--- www.l.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 75.313/96.914/118.516/21.603 ms
```

En la captura següent podeu observar que s'ha fet el *ping*, el client ha resolt per ARP l'adreça de l'encaminador (*router*) local i, aleshores, ha preguntat al servidor DNS (80.58.61.250) per l'adreça de *www.google.com*. El servidor DNS ha contestat indicant que l'adreça IP buscada és *66.102.9.104*. Fixeu-vos que és una consulta DNS que cerca un registre de *tipus A* (hoste).

Podeu observar també que s'ha fet una consulta de resolució inversa en la qual s'ha comprovat que l'adreça IP *66.102.9.104* correspon realment al domini *www.google.com*.



Podeu manipular vosaltres mateixos la captura de la imatge carregant el fitxer de captura del Wireshark que es lliura com a material complementari (podeu baixar el fitxer m7uf1ud1_dhcp_dialeg1.cap al mateix annex).

A continuació podeu observar la llista de text de les quatre trames que contenen informació DNS capturades amb el Wireshark (s'han exportat en format text).

No.	Time	Source	Destination	Protocol	Info
3	0.000449	192.168.1.34	80.58.61.250	DNS	Standard query A www.google.com


```

Frame 3 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AsustekC_15:80:7e (00:17:31:15:80:7e), Dst: XaviTech_7b:ff:1d (00:01:38:7b:ff:1d)
Internet Protocol, Src: 192.168.1.34 (192.168.1.34), Dst: 80.58.61.250 (80.58.61.250)
User Datagram Protocol, Src Port: filenet-rmi (32771), Dst Port: domain (53)
Domain Name System (query)
  [Response In: 4]
  Transaction ID: 0x9d09
  Flags: 0x0100 (Standard query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.google.com: type A, class IN

```

No.	Time	Source	Destination	Protocol	Info
4	0.074927	80.58.61.250	192.168.1.34	DNS	Standard query response

CNAME www.l.google.com A 66.102.9.104 A 66.102.9.147 A 66.102.9.99

Frame 4 (142 bytes on wire, 142 bytes captured)
Ethernet II, Src: XaviTech_7b:ff:1d (00:01:38:7b:ff:1d), Dst: AsustekC_15:80:7e (00:17:31:15:80:7e)
Internet Protocol, Src: 80.58.61.250 (80.58.61.250), Dst: 192.168.1.34 (192.168.1.34)
User Datagram Protocol, Src Port: domain (53), Dst Port: filenet-rmi (32771)
Domain Name System (response)
[Request In: 3]
[Time: 0.074478000 seconds]
Transaction ID: 0x9d09
Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
Queries
 www.google.com: type A, class IN
Answers
 www.google.com: type CNAME, class IN, cname www.l.google.com
 www.l.google.com: type A, class IN, addr 66.102.9.104
 www.l.google.com: type A, class IN, addr 66.102.9.147
 www.l.google.com: type A, class IN, addr 66.102.9.99

No.	Time	Source	Destination	Protocol	Info
7	0.193929	192.168.1.34	80.58.61.250	DNS	Standard query PTR

104.9.102.66.in-addr.arpa

Frame 7 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: AsustekC_15:80:7e (00:17:31:15:80:7e), Dst: XaviTech_7b:ff:1d (00:01:38:7b:ff:1d)
Internet Protocol, Src: 192.168.1.34 (192.168.1.34), Dst: 80.58.61.250 (80.58.61.250)
User Datagram Protocol, Src Port: filenet-rmi (32771), Dst Port: domain (53)
Domain Name System (query)
[Response In: 8]
Transaction ID: 0x6539
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 104.9.102.66.in-addr.arpa: type PTR, class IN

No.	Time	Source	Destination	Protocol	Info
8	0.229144	80.58.61.250	192.168.1.34	DNS	Standard query response PTR

lm-in-f104.google.com

Frame 8 (120 bytes on wire, 120 bytes captured)
Ethernet II, Src: XaviTech_7b:ff:1d (00:01:38:7b:ff:1d), Dst: AsustekC_15:80:7e (00:17:31:15:80:7e)
Internet Protocol, Src: 80.58.61.250 (80.58.61.250), Dst: 192.168.1.34 (192.168.1.34)

User Datagram Protocol, Src Port: domain (53), Dst Port: filenet-rmi (32771)

Domain Name System (response)

[Request In: 7]

[Time: 0.035215000 seconds]

Transaction ID: 0x6539

Flags: 0x8180 (Standard query response, No error)

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

104.9.102.66.in-addr.arpa: type PTR, class IN

Answers

104.9.102.66.in-addr.arpa: type PTR, class IN, lm-in-f104.google.com
