Capítol 4

El Servei DNS
Configuració del servei
Aplicació a les xarxes locals

4.1 El servei DNS (Domain Name Service)

El Servei de Noms de Domini (DNS) consisteix en una base de dades jeràrquica i distribuïda que conté informació de les equivalències entre els nom oficials de domini d'Internet i les adreces IP corresponents. També té la propietat inversa, és a dir, és capaç de resoldre el nom d'un domini a partir de la seva adreça IP. Això s'anomena resolució directa i inversa de noms de domini/IP. Entre altres coses, DNS és necessari per encaminar el correu electrònic de forma coherent, per això la seva gran importància. Qualsevol aplicació que necessiti comunicació amb Internet (la gran majoria) utilitzen DNS per el seu correcte funcionament. Si el DNS es capaç de respondre les peticions de l'aplicació llavors direm que el DNS actua com a Servidor de Noms, però de vegades, el DNS cal que es comuniqui amb altres DNS d'Internet per resoldre un equivalències NOM/IP, llavors diem que actua com a Cau de Resolució de Noms. BIND(v9) (Berkeley Internet Name Domain) de ISC (Internet Systems Consortium) [1] és el paquet de programari de Linux que utilitza la distribució SuSE com a DNS. Pot actuar de les dues formes, com a Servidor de Noms i com a cau de resolució de noms. S'estructura en dues parts:

1. Un fitxer de configuració de nom *named.conf* que podem trobar sota el directori */etc*, el contingut del qual és:

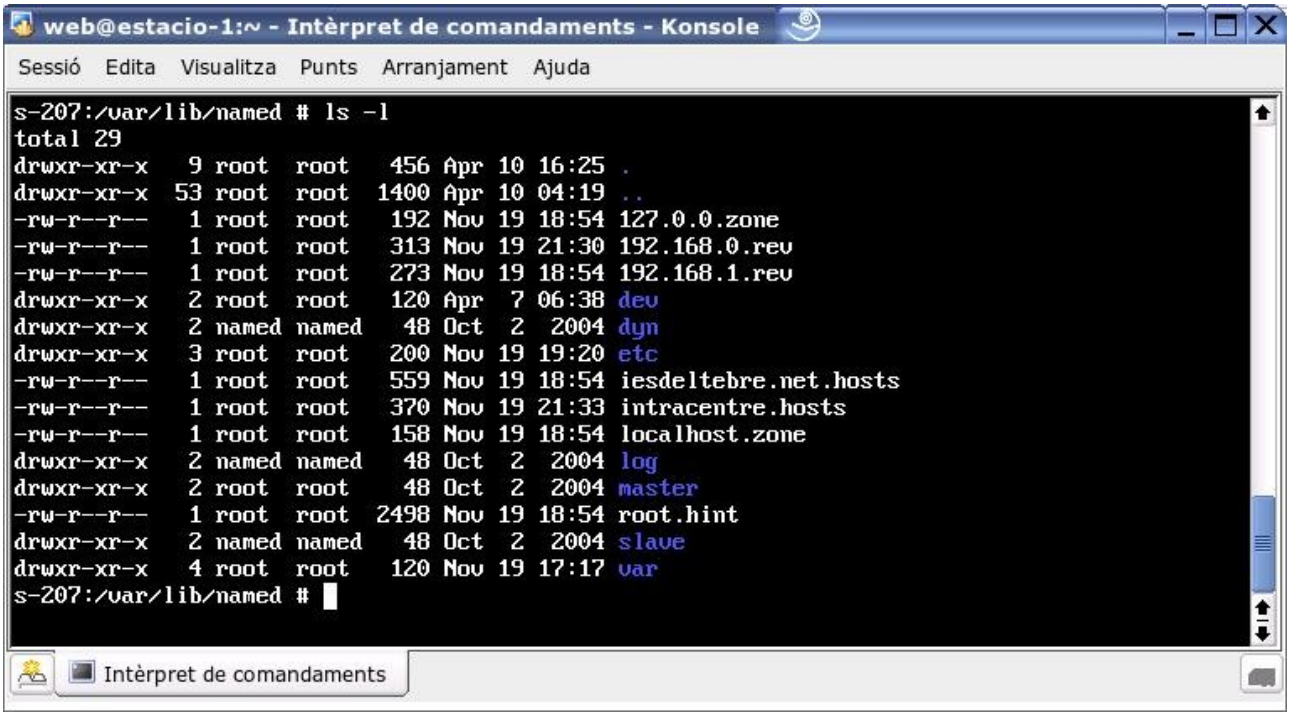
```
options {
        directory "/var/lib/named";
        dump-file "/var/lib/named/log/named_dump.db";
        statistics-file "/var/lib/named/log/named.stats";
        forwarders { 213.176.161.16; 213.176.161.18; };
};
zone "." in {
        type hint;
        file "root.hint";
};
zone "localhost" in {
        type master;
        file "localhost.zone";
};
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/var/lib/named/192.168.0.rev";
        };
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/lib/named/192.168.1.rev";
        };
zone "iesdeltebre.net" {
        type master;
        file "/var/lib/named/iesdeltebre.net.hosts";
        };
zone "intracentre" {
        type master;
        file "/var/lib/named/intracentre.hosts";
        };
```

Com podem veure, el fitxer de configuració està dividit en una secció d'opcions i múltiples seccions referents a les zones. La configuració per defecte (excepte en casos particulars) sol ser bona i únicament cal fer petites variacions.

En el nostre cas, indiquem que el directori on es troben els fitxers de resolució NOM/IP és */var/lib/named* (i altres coses relacionades). Indiquem també quins són els DNS d'ordre superior als que el nostre DNS consulta per resoldre les peticions que és incapaç de satisfer amb la informació que disposa. Una vegada resolta la petició guarda la informació per futures demandes "en memòria", això és el que anomenem cau DNS. En tot moment podem veure quin és el contingut del cau DNS utilitzant la comanda *rndc dumpdb* i observant la sortida al fitxer */var/lib/named/log/named_dump.db*.

Les tres primeres zones definides al fitxer per defecte no necessiten modificacions i es refereixen al servei de noms arrel, la resolució del servidor local i la seva resolució inversa. Les següents zones s'han afegit per fer la resolució de noms en el tram d'IPs 192.168.0.0/24 i 192.168.1.0/24. Els noms de les zones de resolució inverses en cada cas són *iesdeltebre.net.hosts* i *intracentre,hosts*.

2. Un directori de treball, indicat a les opcions, on trobem els fitxers i carpetes que utilitza el servidor per el seu funcionament normal. A la següent figura podem veure un llistat del contingut d'aquest directori:

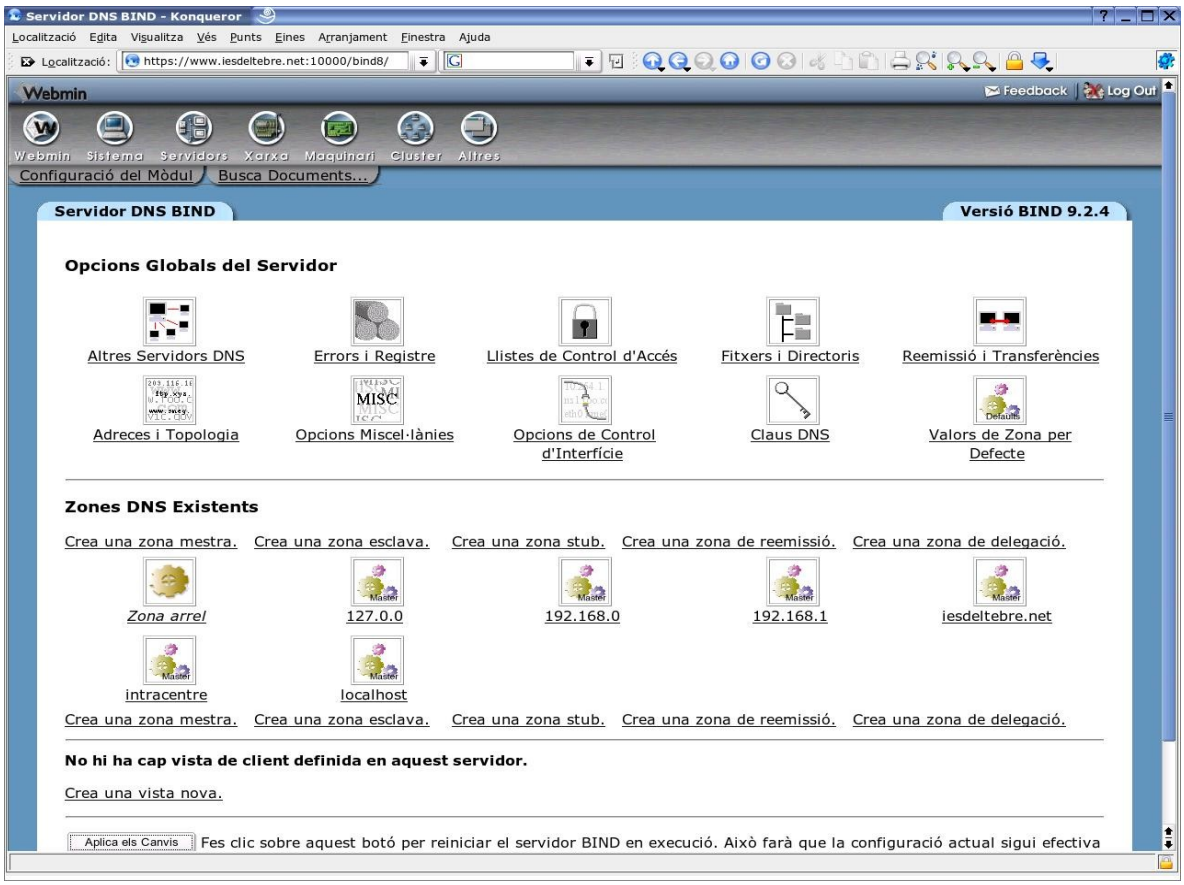


Els fitxers que s'han creat per adaptar el funcionament a les nostres necessitats són:

192.168.0.rev i iesdeltebre.net.hosts
192.168.1.rev i intracentre.hosts

Per ficar en marxa el servei DNS cal executar l'script d'iniciació que trobem sota el directori */etc/rc.d* (en altres distribucions sota */etc/init.d*). l'script s'anomena *named.* Les seves opcions són *start, stop, status, try-restart, restart, force-reload, reload* i *probe*.

Com en el cas del servei SAMBA tenim la possibilitat de configurar el servei DNS amb altres eines com ara el servei WEBMIN. Per fer-ho anem a l'opció de *Servidors -> Servidor DNS Bind* i veurem la següent pantalla d'opcions:



La seva funcionalitat és la mateixa que la línia de comandes, ja que cal donar d'alta un per un tots els parells IP/NOM que es vulguin registrar en el DNS local.

L'altra opció (per SuSE únicament) és utilitzar YAST. Concretament, trobem el servei DNS a *Serveis de Red -> Servidor DNS*. També tenim l'opció de configurar aquí mateix el DNS que utilitzarà per defecte el nostre servidor.

Cal prendre sempre la precaució que el primer DNS sigui la IP del nostre servidor. El fitxer de configuració corresponent a això s'anomena *resolv.conf* i el trobem a /etc. S'ha de semblar a quelcom com això:

```
domain intracentre
nameserver 192.168.0.2          # DNS Local
nameserver 213.176.161.16       # Primer DNS exterior
nameserver 213.176.161.18       # Segon DNS exterior
```

4.2 ¿Per què necessitem definir un DNS propi?

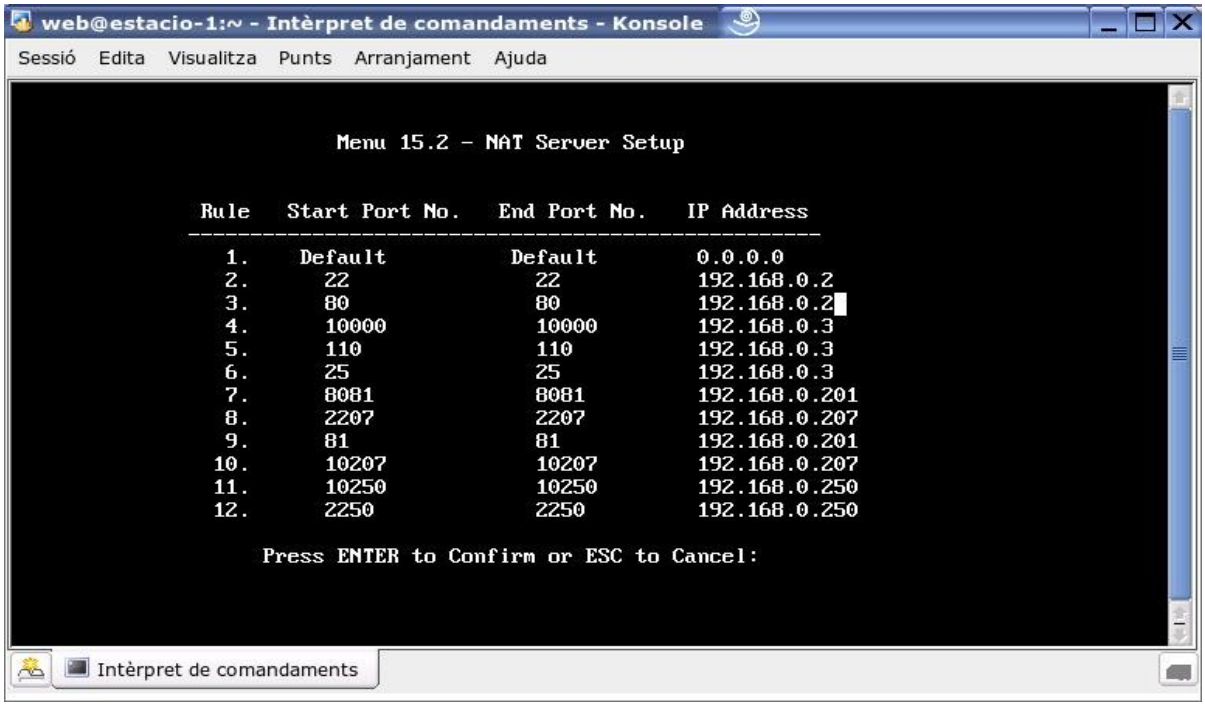
La utilitat d'un DNS propi en una xarxa interna és diversa. Si considerem que el DNS actua com a cau per conservar la informació en memòria de les peticions i la seva resolució i després poder-les servir amb major facilitat als clients, la utilitat esdevé clara: redueix el tràfic a Internet en evitar peticions repetides a servidors DNS exteriors. En realitat la reducció del tràfic és notable (en

empreses “normals” o centres d'ensenyament) si la quantitat de dominis que es tracten en les connexions no és gaire alt (poca diversitat) i es fan moltes peticions als mateixos. Té menys repercussió en casos on la quantitat de dominis visitats és molt diversa i cada domini es visita unes poques vegades (com ara els ciber-cafes).

Per altra banda, encara que el nostre DNS no és “públic” de cara a l'exterior, el podem fer públic de cara als clients de la nostra xarxa interna i resoldre algunes incongruències derivades de tenir una xarxa interna connectada globalment a Internet. Mirem el següent cas:

Un centre d'ensenyament té dos routers (encaminadors) amb dues ADSL per connectar-se a Internet. Disposa d'un servidor web i d'accés SSH a un servidor Linux, tan des de l'interior del centre com des de fora del centre (és a dir des de Internet cap al centre). Això vol dir que tenim registrat un domini d'Internet (per exemple www.iesdeltebre.net) i que aquest s'ha redirigit en els DNS oficials d'Internet cap a una IP que correspon a una de les nostres ADSL (per exemple 217.126.36.161).

El router 1 (que gestiona l'ADSL amb la IP anterior) és el que redirigeix, mitjançant NAT el tràfic que rep des de l'exterior cap al servidor web del centre (d'adreça interna 192.168.0.2). Una configuració NAT típica d'un encaminador pot ser la que s'observa en la següent figura:



Fins aquí tot és relativament fàcil. El primer problema el trobem si volem que els usuaris de la xarxa interna es connectin al servidor. Les opcions que tenim són diverses però no equivalents de cara a l'usuari final.

Per exemple, podem demanar als usuaris que des de dins del centre utilitzin l'adreça IP per fer les connexions enlloc del nom i que des de l'exterior del centre facin servir el nom del domini.

Altra opció és assignar nom i IP internament a tots els clients, és a dir que als fitxers hosts (o lmhosts) dels clients s'inclogui una entrada com aquesta:

```
127.0.0.1       localhost
# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback
```

```
fe00::0         ipv6-localnet
ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
192.168.0.10    estacio-1.intracentre       estacio-1
192.168.0.2     www.iesdeltebre.net     s-207
```

La primera proposta és incòmoda per els usuaris de la xarxa i la segona poc viable si la quantitat d'ordinadors a configurar és molt gran. Cal buscar una solució viable per la quantitat de feina i que sigui transparent per l'usuari.

Encara hi ha una tercera solució que és utilitzar el router 2 com a porta de sortida per visitar la nostra pròpia pàgina web. Evidentment això té poc sentit i provoca un augment del tràfic d'Internet absolutament innecessari.

Mirem com configurem el nostre servidor i què cal fer en els clients de la xarxa per evitar aquest problema. Recordem que al fitxer de configuració s'han indicat 4 zones "mestres" que no estaven per defecte a la configuració estàndard de BIND. Aquest zones estan indicades per 4 fitxers que es troben sota el directori de treball de BIND (*/var/lib/named*). A continuació es pot observar amb deteniment què contenen cada parell de fitxers de resolució de zona directa i inversa.

Comencem per 192.168.0.rev i *iesdeltebre.net.hosts*. Mirem el contingut dels fitxers:

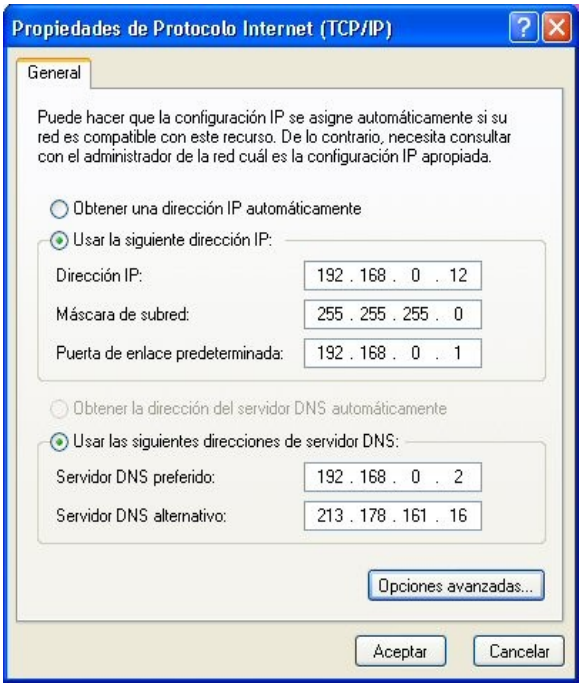
192.168.0.rev	***iesdeltebre.net.hosts***
$ttl 38400	$ttl 38400
0.168.192.in-addr.arpa. IN SOA s-207. ocastell (	iesdeltebre.net. IN SOA s-207. ocastell (
2003062504	2003062502
10800	10800
3600	3600
604800	604800
38400)	38400)
0.168.192.in-addr.arpa. IN NS s-207.	iesdeltebre.net. IN NS s-207.
2.0.168.192.in-addr.arpa. IN PTR s-207.iesdeltebre.net.	s-207.iesdeltebre.net. IN A 192.168.0.2
2.0.168.192.in-addr.arpa. IN PTR iesdeltebre.net.	iesdeltebre.net. IN CNAME s-207
	www.iesdeltebre.net. IN CNAME s-207

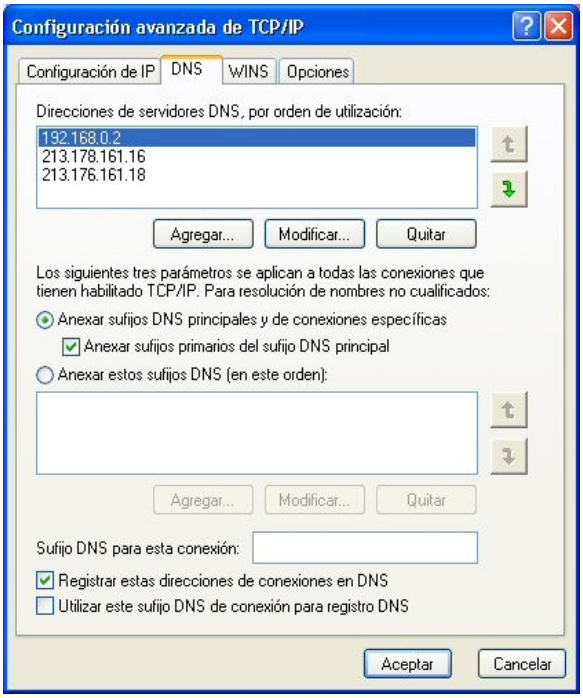
Aquests fitxers contenen la resolució de parells NOM/IP corresponents al tram de xarxa 192.168.0.0/24. Això vol dir que en ficar un nom relacionat amb una IP dins d'aquest tram el servidor DNS serà capaç de resoldre les peticions de clients assignant el NOM a partir d'una IP del tram o assignant la IP a partir d'un NOM. En tots dos fitxers apareix l'associació entre *iesdeltebre.net* i la IP 192.168.0.2.

Així, en fer la consulta al DNS de la IP 192.168.0.2 aquest respondrà que és *iesdeltebre.net*. De la mateixa manera si fem un ping, per exemple, a *iesdeltebre.net* ens respondrà la màquina amb IP 192.168.0.2. Això és just el que volíem aconseguir.

Ara bé, aquesta solució s'ha de aplicar als clients. Per fer-ho cal que indiquem en la seva

configuració de xarxa que el primer DNS que han de consultar és el nostre servidor DNS de la xarxa interna:





El nostre servidor disposa de dues targetes de xarxa i, per defecte, BIND emet i rep trànsit de totes i cap a totes les interfícies (a no ser que indiquem el contrari amb un filtre de paquets, com per exemple amb *iptables*). Així que ens interessa que el nom del nostre servidor s'associï a una IP "possible i factible" en cada tram.

Ens cal crear fitxers de configuració per cada tram de xarxa que gestioni el nostre servidor. Per al tram d'IPs 192.168.1.0/24 els fitxers de configuració són *192.168.1.rev* i *intracentre.hosts*. En aquestes zones definirem les IPs i els noms corresponents que volem que els clients d'aquest tram utilitzin. Aquests fitxers contenen la següent informació:

192.168.1.rev	***intracentre.hosts***
$ttl 38400 1.168.192.in-addr.arpa. IN SOA s-207. ocastell (2003062504 10800 3600 604800 38400) 1.168.192.in-addr.arpa. IN NS s-207. 1.1.168.192.in-addr.arpa. IN PTR s-207.iesdeltebre.net. 1.1.168.192.in-addr.arpa. IN PTR iesdeltebre.net.	$ttl 38400 intracentre. IN SOA s-207. ocastell (2003062502 10800 3600 604800 38400) intracentre. IN NS s-207. iesdeltebre.net. IN CNAME s-207 www.iesdeltebre.net. IN CNAME s-207

Els clients del tram IP 192.168.1.0/24 seguiran la configuració que ja s'ha indicat en el capítol anterior: la passarel·la, el DNS i el WINS han de ser la IP del servidor 192.168.1.1.

La configuració dels clients Linux és idèntica a la exposada abans: cal modificar el fitxer *resolv.conf* per assegurar que el primer DNS és el nostre servidor (192.168.0.2 o 192.168.1.1).

Segons el tram d'IP a que pertany el client tindrem:

192.168.0.0/24	***192.168.1.0/24***
domain intracentre nameserver 192.168.0.2 nameserver 213.176.161.16 nameserver 213.176.161.18	domain intracentre nameserver 192.168.1.1

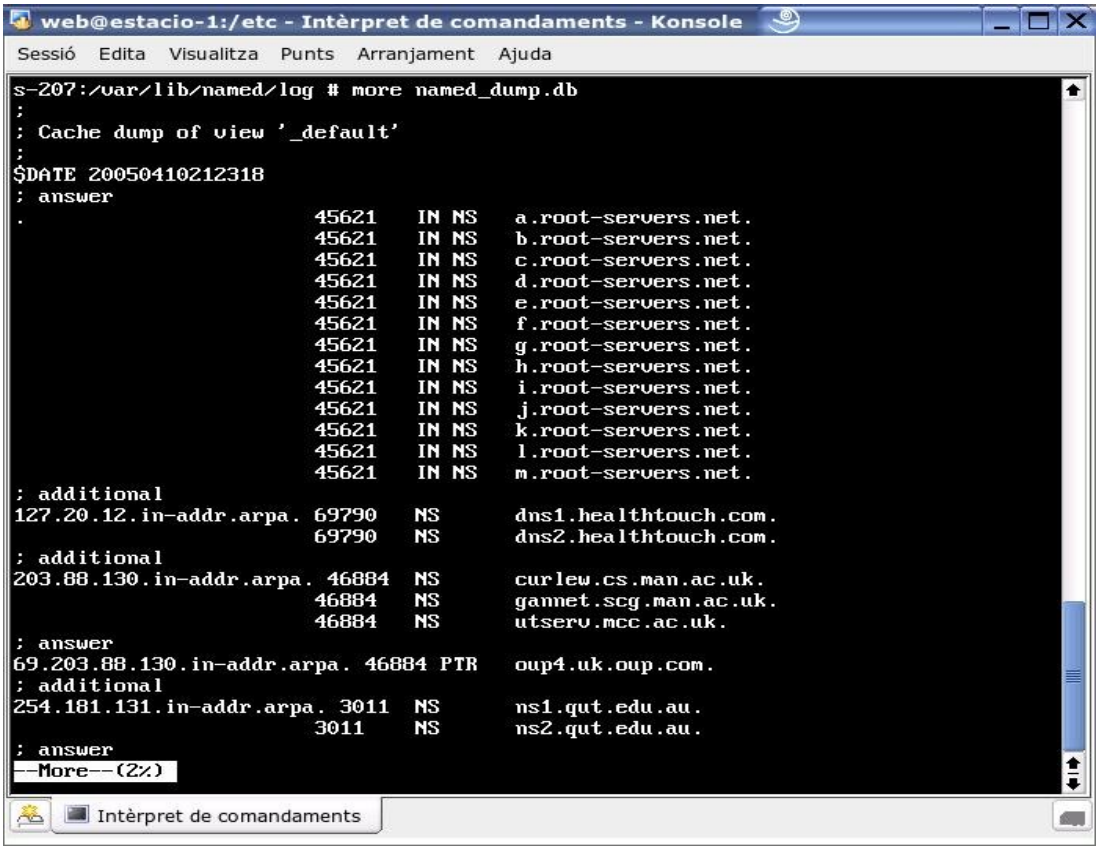
4.3 Comprovació del servei

Per veure el correcte funcionament del DNS farem les següent pràctiques al taller:

1. Per veure el funcionament del cau DNS utilitzarem la comanda *rndc* de la següent manera:

   s-207:/var/lib/named/log # rndc dumpdb

   Això extreu tota la informació del cau en memòria i la guarda aun fitxer situat (segons *named.conf*) en el directori */var/lib/named/log* i que s'anomena *named_dump.db*. Mirem el seu contingut per entendre com funciona el cau:



   Com es pot veure, el que fa BIND es conservar totes les peticions i respostes dels dominis que s'han visitat i dels DNS que s'han utilitzat per aconseguir la resposta corresponent a una demanda.

2. Per veure el funcionament del la resolució interna dels noms de domini corresponents a la nostra xarxa utilitzarem la comanda *ping*. Primer utilitzarem un client on el primer

DNS no és el nostre servidor i farem un ping a www.iesdeltebre.net: anotem la sortida. En un pas posterior ficarem el nostre servidor DNS en primera posició: anotem la sortida i compararem els resultats. Ha de ser quelcom així:

```
s-207:/var/lib/named/log # ping www.iesdeltebre.net
PING www.iesdeltebre.net (217.126.56.181) 56(84) bytes of data.
64 bytes from 181.Red-217-126-56.pooles.rima-tde.net (217.126.56.181): icmp_seq=1 ttl=155 time=0.650 ms
```

```
s-207:/var/lib/named/log # ping www.iesdeltebre.net
PING s-207.iesdeltebre.net (192.168.0.2) 56(84) bytes of data.
64 bytes from s-207.intracentre (192.168.0.2): icmp_seq=1 ttl=64 time=0.071 ms
```

És evident el bon funcionament, tal com ens calia esperar. Si fem atenció als resultats i comparem els temps de resposta veurem que la resolució local es de l'ordre de 10 vegades més ràpida. Si ho multipliquem pel nombre de peticions diàries que ens estalviem cap a Internet veiem una vegada més la utilitat del DNS.

Referències:

[1] Pàgina oficial de BIND a la ISC: http://www.isc.org/index.pl?/sw/bind/