UF1. Servei de noms i configuració automàtica

NF1. Instal·lació i configuració DNS

Índex

1. Introducció

Dins d'aquest apartat veurem com **dotar a la nostra xarxa local** amb TCP/IP **d'un servei de noms** imprescindible per al **correcte funcionament dels serveis que implementarem més endavant**.

El servei DNS va aparèixer l'any 1983, va sorgir per la **necessitat d'emmagatzemar de forma estructurada els noms** de tots els serveis connectats a Internet.

Inicialment es guardava en cada màquina un arxiu anomenat `hosts.txt` que **contenia tots els noms de domini coneguts**, però a mesura que Internet va anar creixent, la mida del fitxer també, això provocava una sèrie de problemes que no es podien assumir.

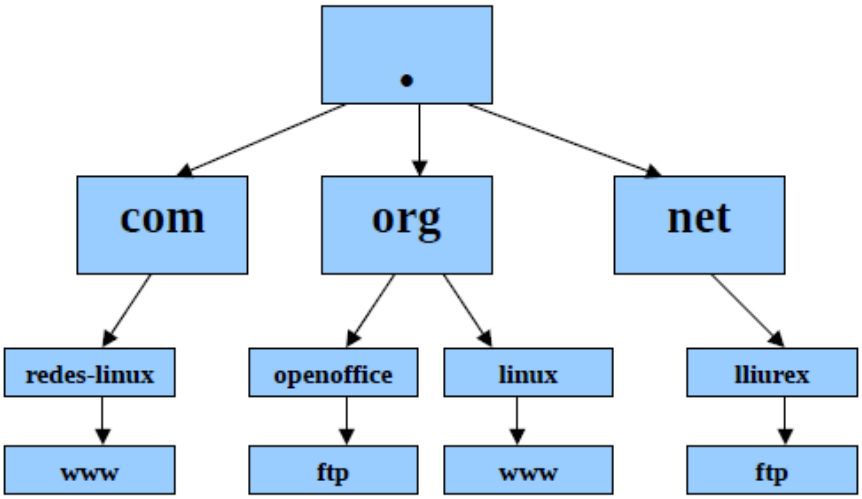
Llavors va ser quan Paul Mockapetris va **publicar els estàndards (RFC 882 i 883)** que defineixen el que avui coneixem com **DNS**.

2. L'espai de noms de domini

El servei **DNS** està format per una **base de dades distribuïda**, és a dir, que està **emmagatzemada en diverses màquines connectades** en xarxa (poden estar en el mateix lloc físic o distribuïdes per la xarxa), això permet accedir a les dades des de diferents màquines. En aquesta base de dades **s'emmagatzemen associacions de noms de dominis i direccions IP**.

La **base de dades de DNS està classificada per noms de domini**, on **cada nom de domini és una rama d'un arbre invertit** anomenat espai de noms de domini. L'arbre comença pel node arrel al nivell superior, i per baix ell poden existir un número indeterminat de nodes de nivell inferior (normalment s'utilitzen fins un màxim de 5 nivells). Exemple `lliurex.cult.gva.es` està format per 4 nivells.

Els nodes s'identifiquen mitjançant noms no nuls, és a dir, que han de tenir un número determinat de caràcters (màx. 63), a excepció del node arrel que s'identifica mitjançant un nom nul (0 caràcters). El **nom complet d'un node** està format pel **conjunt de noms que formen la trajectòria** des d'aquest node fins el node arrel.



Els diferents **servidors DNS** que existeixen a la xarxa **emmagatzemen la informació relativa als noms de domini DNS en registres de recursos**. Un determinat servidor DNS tindrà aquells registres de recursos que li permetin respondre a les peticions de noms relatives als noms de domini sobre els que té autoritat.

3. La xarxa TCP/IP sense serveis de noms

Una **estructura de xarxa** està formada bàsicament per **elements que es comuniquen entre ells**.

En el **nivell més baix**, els diferents sistemes **es reconeixen utilitzant l'adreça MAC** de la targeta de xarxa, formada per sis parells de dígits hexadecimals, els tres parells inicials poden repetir-se, doncs indiquen el fabricant, i els altres tres són diferents, composant una 'matrícula' única per a cada dispositiu.

Per exemple, podem observar l'adreça MAC de la placa de xarxa del nostre Linux executant:

```
root@servidor-primari:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:07:cc:27
          inet addr:192.168.203.99  Bcast:192.168.203.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe07:cc27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1041 errors:0 dropped:4 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:97505 (97.5 KB)  TX bytes:13022 (13.0 KB)
```

indicada com a '**HWaddr'** i de valor **08:00:27:07:cc:27**, podem 'descobrir' el fabricant destriant els tres primers parells:

08:00:27 - Oracle VM VirtualBox, Inc

Aquests **tres primers dígits són 'propietat' de l'empresa Oracle VM VirtualBox**, i ha d'identificar sempre les seves plaques de xarxa, de manera que comencin per aquestes xifres.

En el cas de les xarxes TCP/IP, tenim uns **identificadors de més alt nivell**, **l'adreça IP**, que també ha d'ésser únic per a cada element de la xarxa, **i el nom de la màquina** (també anomenat nom de host).

El tipus d'adreçament utilitzat dins les xarxes 'tancades' amb TCP/IP (altrament dites intranets) **està definit per unes normes**, per evitar 'trepitjar' adreces utilitzades a Internet.

10.0.0.0 - 10.255.255.255 (una xarxa classe A)
172.16.0.0 - 172.31.255.255 (16 xarxes classe B)
192.168.0.0 - 192.168.255.255 (256 xarxes classe C)

En les empreses s'acostuma a utilitzar el rang 192.168.0.x, la primera de les 256 xarxes C disponibles.

Així doncs, **si un equip amb l'adreça 192.168.70.20 vol accedir als serveis d'una altra**, **inicialment ha de conèixer la seva adreça IP i es veu obligat a utilitzar-la** per fer-ne referència des de qualsevol aplicació.

Per exemple, si **una estació** amb l'adreça 192.168.70.20 **vol consultar la pàgina web** principal del servidor linux, només **hi podrà accedir des del navegador** indicant la URL:

`http://192.168.70.1/`

Per defecte no podrem adreçar-nos a les màquines pel seu nom, i això ens obligaria a aprendre de memòria totes les adreces IP de les màquines que ens donen serveis.

Anem a veure **com podem preparar un servei de noms per poder dotar els equips de la xarxa de noms més 'amigables'** i permetre configurar serveis referint-nos a aquests noms.

4. Cal un servei de noms a la xarxa

El servei de noms es presenta com a **imprescindible bàsicament per dues raons**:

1. Podem **accedir als serveis** dels equips **adreçant-nos a ells amb un nom 'clar'** i fàcil de recordar pels usuaris.
2. **Fem les configuracions dels serveis utilitzant aquests noms** en comptes de l'adreça IP, aconseguint una **flexibilitat molt interessant**.

Per exemple, si teniu **configurat en els navegadors de 400 màquines** de la xarxa del centre, la **URL d'accés al fitxer** de configuració automàtica **del proxy** així:

`http://192.168.70.1/proxy.pac`

i us **arriba un servidor molt més potent amb una nova configuració** més recomanable, caldria canviar la configuració de totes les estacions, ja que la nova màquina té la IP 192.168.70.2... i la nova URL seria:

`http://192.168.70.2/proxy.pac`

això implica molta feina!

En canvi, **si utilitzem el servei de noms**, **podríem configurar-ho amb un nom**, de manera que si ens cal canviar el motor del servei i aquest té una altra IP, **només cal modificar la referència amb el mateix nom la nova IP**.

Seguint l'exemple, si hi ha servei de noms, la nova URL que podríem utilitzar seria així:

`http://proxy.intracentre/proxy.pac`

de manera que **només cal canviar dins el servei de noms, la IP que fa referència a 'proxy.intracentre'** de la 192.168.70.1 (antiga) a la 192.168.70.2. No caldrà tocar mai més la configuració de les 400 estacions una per una...

Hem vist amb un exemple alguns dels avantatges que ens pot oferir el servei de noms, n'hi ha molts més que ja anireu descobrint amb la pràctica.

5. Característiques del servei DNS d'una xarxa local 'tancada'

El **servei de noms** dins les xarxes TCP/IP **s'anomena DNS (Domain Name System)** i **es pot implementar de diferents maneres**, depenent del tipus de servei que ha de donar.

Bàsicament hi ha **dos tipus de configuració** dels serveis de DNS:

1. **El DNS per al treball a Internet**, totalment públic. És l'**encarregat d'escampar les adreces d'aquest domini** (un nom vàlid a Internet assignat per 'Internic', del tipus `nom.es` per exemple) **i resoldre les peticions adreçades a altres dominis**.

   Dins aquest DNS només hi poden aparèixer les IP totalment vàlides a Internet, i cal una configuració força acurada del refresc de les modificacions que s'hi puguin fer i la transferència d'aquesta informació entre servidors.

2. **El DNS per al treball dins una xarxa local**, totalment privat. Serà l'encarregat de resoldre **només les peticions de nom-IP / IP-nom de la seva xarxa**.

   Aquest DNS **no pot tenir mai cap relació directa amb Internet**, les adreces que ell coneix no es poden publicar a l'exterior.

El servei que implementarem serà el segon tipus, però amb un petit '**afegit**', donat que volem que

les màquines de la xarxa interna puguin accedir a Internet.

El nostre DNS intern, que no pot 'publicar' cap de les seves adreces a Internet, **serà 'client'** mitjançant 'forwarding' **del DNS Internet de l'Institut de l'Ebre**. Així, **si el nom demanat no el coneix directament, passarà la petició i emmagatzemarà la resposta dins una petita cache**, per servir-la quan faci falta.

6. Implementació del servei DNS

6.1. Requeriments de programari

El **servei DNS el fa efectiu el 'paquet' `bind`**, que podeu descarregar-lo lliurement des de la web. Si heu seguit correctament la instal·lació del sistema operatiu, ja teniu en el sistema els components necessaris per posar en marxa el servei, comproveu-ho amb el programa de gestió de paquets, verificant que apareixen llistats els següents paquets: `bind9`, `bind9-doc` i `bind9utils`.

Per comprovar si està instal·lat o no, ho podeu comprovar amb la comanda:

```
dpkg -L bind9
```

Si no està instal·lat, apareixerà el següent missatge:

```
alumne@primary-server:~$ dpkg -L bind9
dpkg-query: package 'bind9' is not installed
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

Per instal·lar el servei DNS, cal instal·lar els paquets bind9 i dnsutils amb la comanda:

```
apt-get install bind9 bind9-doc bind9utils
```

Una vegada instal·lat, en /etc/bind9/ es poden trobar els següents arxius:

```
alumne@primary-server:/etc/bind$ ls
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
```

L'execució d'un servidor DNS utilitzant `bind9` implica l'execució del **procés named, el seu arxiu de configuració és `named.conf`** (doneu-li una ullada). Aquest fitxer està format per un conjunt de sentències i comentaris, les sentencies finalitzen amb el caràcter ";", aquestes sentències poden estar contingudes en claus { }. La primera línia d'aquest arxiu inclou l'arxiu **`named.conf.options`** (on tenim les opcions globals del servidor), i les dos següents inclouen els **`named.conf.local` i `named.conf.default-zones`** (on es defineixen les nostres zones locals en el servidor de noms), d'aquesta manera ens estalviem tenir que modificar l'arxiu `named.conf`.

```
  GNU nano 2.2.6               File: named.conf

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

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Per comprovar si **tenim en execució el servei DNS** a la nostra màquina ho podem fer instal·lant prèviament el paquet nmap, i executant la comanda **`nmap -sU localhost -p 53`**:

```
alumne@primary-server:~$ sudo nmap -sU localhost -p 53
sudo: unable to resolve host primary-server

Starting Nmap 6.40 ( http://nmap.org ) at 2015-09-12 11:43 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Es pot observar com que aquesta execució mostrarà si el port 53 està obert o tancat, indicant si està obert que el servei DNS està en funcionament.

Per a configurar el nostre *caching only server*, hem de considerar que les preguntes en primer lloc les resoldrem nosaltres però com que és evident que no tenim la resposta, s'haurà de redirigir la pregunta a servidors de DNS en la xarxa. Per a això, és interessant considerar els de serveis com OpenDNS (http://www.opendns.com/opendns-ip-addresses/) que són les IP: 208.67.222.222 i 208.67.220.220 o bé serveis com els de Google (https://developers.google.com/speed/public-dns/?csw=1) que responen les IP: 8.8.8.8 i 8.8.4.4.

6.2. Estructura dels fitxers del servidor DNS

Els **fitxers que composaran la configuració bàsica del nostre servidor** DNS, suposant que treballarem dins la xarxa **192.168.70.x** amb el nom **informaticaASIX2.com**, són:

`/etc/bind/named.conf.options:` Conté la configuració bàsica del DNS. El contingut d'aquest fitxer serà el següent:

```
options {
      directory "/var/cache/bind";
      forward only;
      forwarders {
            192.168.202.2;
            8.8.8.8;
      };
      auth-nxdomain no;
```

```
      listen-on-v6 { any;};
};
```

Aquest fitxer ens marca les **opcions generals del servei** de DNS mitjançant la sentència **options**, dins d'aquesta sentència podem trobar diferents declaracions:

- Una d'aquestes és la de configuració dels **forwarders** que **resoldran totes les peticions externes a la xarxa**, és a dir, totes aquelles peticions que no resolgui el DNS local seran re-enviades al servidor que indiquem mitjançant la @IP. Per exemple:

```
forwarders {
      // OpenDNS servers
      208.67.222.222;
      208.67.220.220;
      // Podríem incloure el nostre ISP/router -verificar la IP-
      192.168.1.1;
};
```

- **Forward only** significa que les consultes DNS externes només s'enviaran als forwarders:

```
forward only;
```

- Amb **directory** indiquem el directori on s'emmagatzemen els arxius temporals generats pel procés named:

```
directory "/var/cache/bind";
```

- **dnssec-validation** serveix per activar les extensions de seguretat del DNS, per a més informació https://ca.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- **Allow-query** permet fer consultes DNS a totes les màquines de la xarxa que indiquis. Per exemple,

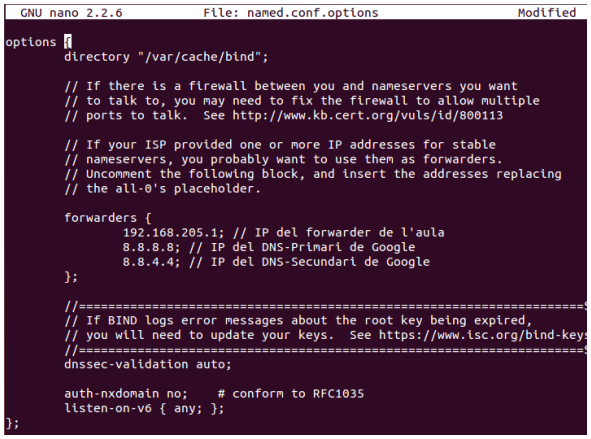
```
allow-query {192.168.70/24;};
```

- De la mateixa manera amb **blackhole** deneguem les consultes DNS a totes les màquines de les xarxes indicades en una acl. Per exemple:

```
acl xarxes {192.168.0.0/16;192.168.70.1;};
blackhole {xarxes;};.
```

- **Auth-nxdomain** permet configurar el bit AA, que indica si el nostre servidor està autoritzat a respondre sobre consultes de la seva zona.

Exemple de configuració del fitxer `/etc/bind/named.conf.options`:



/etc/bind/named.conf.local: Conté la configuració de les zones locals del DNS (directa i inversa).

```
zone "informaticaASIX2.com" {
      type master;
      file "/etc/bind/db.ASIX2.hosts";
      notify yes;
};
zone "70.168.192.in-addr.arpa" {
      type master;
      file "/etc/bind/192.168.70.rev";
      notify yes;
};
```

En el **segon fitxer**, les 'zones' indiquen el **camí dels arxius que conformen la base del DNS**, en aquest cas tant senzill, només hi ha una zona directa definida en el fitxer **db.ASIX2.hosts** i la seva corresponen inversa al **192.168.70.rev.**

/etc/bind/db.ASIX2.hosts: Zona directa, utilitzada per trobar les IP partint dels noms.

El contingut d'aquest fitxer serà el següent:

```
$TTL  604800
informaticaASIX2.com. IN SOA servidor-primari.informaticaASIX2.com. root.informaticaASIX2.com. (
               1 ; Serial
               604800 ; Refresh
               86400 ; Retry
               2419200 ; Expire
               604800 ) ; Negative Cache TTL
informaticaASIX2.com.          IN      NS      servidor-primari.
informaticaASIX2.com.          IN      A       192.168.70.1
servidor-primari               IN      A       192.168.70.1
pc01.informaticaASIX2.com      IN      A       192.168.70.21
www                            IN      CNAME   servidorx
```

Cada zona comença amb el registre de recursos d'Inici d'Autoritat o SOA (start of authority). Els camps que conté són els següents:

- **Propietari:** nom de domini de la zona, en el nostre cas `informaticaASIX2.com`, es pot utilitzar el nom o el caràcter @, en aquest cas agafarà com a nom de la zona el definit en el fitxer named.conf.local, per tant, ha de coincidir.
- **Tipus de registre:** SOA.
- **Servidor Mestre:** Indica el nom del servidor DNS mestre.
- **Persona responsable:** Conte la direcció de correu electrònic del responsable de la zona. En aquesta direcció s'utilitza el punt en lloc de @. En el nostre cas root.informaticaASIX2.com.
- **Número de serie (serial number):** Número de versió de la zona. S'utilitza com a referència per als servidors secundaris per a saber quan han de fer una actualització de la seva base de dades de la zona. Si el nº de sèrie del servidor secundari és menor que el nº del primari, significa que el primari ha canviat la informació de la zona. Aquest nº l'ha d'incrementar manualment l'administrador de la zona cada vegada que realitza algun canvi en el registre de la zona(al servidor primari). S'acostuma a utilitzar el format AAAAMMDDNN (any, mes, dia i número de canvi respecte el dia en curs, encara que també es pot utilitzar només NN, és a dir, el número de canvi.
- **Actualització (Refresh Time):** Indica cada quan temps (en segons) un servidor secundari ha de contactar amb el primari per a comprovar els canvis de la zona.

- **Reintents (Retry Time):** Si la transferència de zona ha fallat, aquest camp indica el temps (en segons) que espera el servidor secundari abans de tornar a intentar-ho.
- **Caducitat (Expire Time):** Indica el temps de caducitat (en segons), de la informació de la zona en un servidor secundari.
- **TTL mínim:** Indica el temps de validesa del registre SOA, és a dir, número de segons que la informació sobre el registre és manté en el servidor de noms de domini (caché).

Els registres mínims que utilitzarem són:

- **IN NS** Estableix l'equip servidor de noms (DNS) autoritzat per a la zona del domini `informaticaASIX2.com`. Cada zona ha de contenir registres indicant tant els servidors primaris com secundaris, per tant, cada zona ha de tenir com a mínim un registre NS.

  NOTA: Alternativament, si hem utilitzat una arrova per indicar el nom del domini, podem no posar, el nom del domini al començament.
- **IN A** Estableix una correspondència entre una @IP i un nom de domini, en el nostre cas pc01. Cada registre A identifica un nom de màquina, i el client DNS pot obtenir a través d'ell la seva direcció IP.

  Caldrà doncs completar amb entrades IN A la definició de totes les màquines de la nostra xarxa, afegint per exemple:

  ```
  secretaria.informaticaASIX2.com. IN A 192.168.70.120
  biblioteca.informaticaASIX2.com. IN A 192.168.70.121
  ...
  ```
- **IN CNAME** Defineix un 'àlies' com a segon nom reconegut d'una IP ja definida anteriorment. En el nostre cas `servidor-primari.informaticaASIX2.com` serà `www.informaticaASIX2.com`.

IMPORTANT: Si es posa el nom de la zona cal **no oblidar-se del punt final!** Si no hi ha punt es considera una abreviatura, per exemple:

`www.iesebre.com IN A 192.168.70.1`

equival a `www.iesebre.com.iesebre.com`

Atenció amb **la separació entre els ítems**, s'ha de fer obligatòriament amb tabulador.

`/etc/bind/192.168.70.rev`: Zona inversa, utilitzada per trobar els noms partint de l'adreça IP.

El contingut d'aquest fitxer serà el següent:

```
$TTL  604800
@      IN     SOA    servidor-primari.informaticaASIX2.com.  root.informaticaASIX2.com. (
              1
              604800
              86400
              2419200
              604800 )
@                                IN     NS     servidor-primari.
1.70.168.192.in-addr.arpa.       IN     PTR    informaticaASIX2.com.
1.70.168.192.in-addr.arpa.       IN     PTR    servidor-primari
21.70.168.192.in-addr.arpa.             IN     PTR    pc01.informaticaASIX2.com
```

També es pot definir de la següent manera (potser és més entenedora):

```
$TTL  604800
@      IN     SOA    servidor-primari.informaticaASIX2.com.  root.informaticaASIX2.com. (
              1
              604800
              86400
              2419200
              604800 )
@      IN     NS     servidor-primari.
1      IN     PTR    informaticaASIX2.com.
1      IN     PTR    servidor-primari
21     IN     PTR    pc01.informaticaASIX2.com
```

Els **paràmetres inicials són idèntics al de la zona directa** i **han de coincidir** també exactament totes les entrades IP amb els noms definits. **Si es modifica el directe caldrà mantenir aquest també actualitzat**.

Els registres mínims que utilitzarem són (sense tenir en compte els definits anteriorment):

- **IN PTR** Aquest registre és un recurs punter i fa el contrari que el registre A, només s'utilitza en la resolució inversa.

Existeixen altres registres que no utilitzarem: el **MX (mail exchange)** per indicar les màquines encarregades de lliurar el correu dins del domini i el **SRV** per indicar la ubicació dels servidors per a un servei.

6.3. El per què de la notació in.addr.arpa

Com ja sabeu **la resolució dels noms de domini es fa mitjançant consultes que van de dreta a esquerra**, per tant, es lògic pensar que per resoldre @IP es segueix la mateixa direcció. El domini arrel en **aquest cas s'anomena in-addr.arpa** a diferència dels noms de domini que comencen per '.'

Per exemple **si tenim la @IP 192.168.70.1, el servidor de noms** buscarà els servidors arpa, passarà als in-addr.arpa, llavors a **192.in-addr.arpa** i així fins arribar a 1.70.168.192.in-addr.arpa fins trobar el registre buscat. Per tant podem afirmar que s'utilitza una notació puntejada inversa, de fet **és lògic utilitzar-la ja que els primers octets d'una @IP identifiquen la xarxa a la qual pertany** i la diferència d'altres xarxes.

Podeu veure com **mantenir-lo de forma més còmoda via Web** (aplicació Webmin). Heu de tenir instal·lats el **paquets webmin i webmin-bind**. S'accedeix via web amb la direcció `https://localhost:10000/`. També existeix una aplicació gràfica als repositòris anomenada **GADMIN-BIND**.

6.4. Comandes per comprovar la configuració i modificacions inicials

1. **named-checkconf:** comprovem la sintaxis de named.conf i els fitxers que inclou. Amb el paràmetre `-z` es pot obtenir informació addcional.
2. **named-checkzone:** comprovem la sintaxis dels arxius de zona. Per exemple:

   ```
   named-checkzone informaticaASIX2.com /etc/bind/db.ASIX2.hosts
   ```

   Es pot utilitzar el paràmetre `-D` per debuggar si tots els noms de màquina s'han creat correctament.
3. **dig:** Permet realitzar consultes a un servidor DNS, s'acostuma a utilitzar per detectar

problemes de configuració. Per exemple:

```
dig informaticaASIX2.com
```

o

```
dig 0.70.168.192.in-addr.arpa
```

```
dig -t PTR 1.70.168.192.in-addr.arpa
```

4. **host:** Permet fer cerques dins del DNS, s'utilitza per convertir noms a @IP i al contrari, per tant podrem comprovar si funcionen la zona directa i inversa.
5. **nslookup:** És un altra forma de fer consultes al servidor DNS. Per exemple:

   ```
   nslookup servidor-primari.informaticaASIX2.com
   ```

   o

   ```
   nslookup www.informaticaASIX2.com
   ```

6. Podem veure els fitxers log del sistema amb la comanda

   ```
   tail -f /var/log/syslog | grep named
   ```

   on s'ha de poder veure els següent:

   ```
   named[6738]: received control channel command 'querylog'
   named[6738]: query logging is now on
   ```

7. **rndc:** Amb aquesta comanda podem consultar l'status del servidor DNS, per exemple amb:

   ```
   rndc status
   ```

8. **dnstop:** És una comanda de monitorització, mostra les peticions dns a temps real i de qui provenen, s'ha d'indicar la targeta de xarxa per on rebrem les peticions, per exemple:

   ```
   dnstop eth1
   ```

Per últim s'ha de tenir present de modificar l'arxiu `/etc/resolv.conf` **per a que la màquina busqui el domini** que s'ha creat, s'han d'incloure les següents línies:

```
search informaticaASIX2.com
nameserver 192.168.70.1
```

IMPORTANT: El contingut que escriguis al fitxer `/etc/resolv.conf` s'esborra al reiniciar, caldrà fer alguna modificació al sistema per fer-los permanents.

6.5. Posada en marxa del servei de noms

En aquests moments només cal assegurar que el servei de noms 'named (bind9)' **es posarà en marxa cada cop que arrenqui el servidor** i s'aturarà correctament quan apaguem l'equip.

Per defecte **la instal·lació** del paquet **crea uns 'links'** dins de tots els directoris **/etc/rc?.d/** indicant el seu ordre d'arrencada i el seu nom. Si el servidor arrenca normalment amb el nivell 2 només cal anar al directori **/etc/rc2.d** i crear el link **S15bind9** (per exemple) amb l'ordre (en el cas que no estigui creat):

```
cd /etc/rc02.d/
```

```
ln -s ../init.d/bind9 S15bind9
```

Per comprovar si s'ha creat correctament, cal anar al directori /etc/rc2.d/ i llistar el directori per

observar si s'ha creat l'enllaç simbòlic:

```
alumne@servidor-primari:/etc/rc2.d$ ls -l
total 4
-rw-r--r-- 1 root root 677 jun 15 05:31 README
lrwxrwxrwx 1 root root  15 sep 12 11:30 S15bind9 -> ../init.d/bind9
lrwxrwxrwx 1 root root  20 sep  9 22:21 S20kerneloops -> ../init.d/kerneloops
lrwxrwxrwx 1 root root  15 sep  9 22:21 S20rsync -> ../init.d/rsync
lrwxrwxrwx 1 root root  27 sep  9 22:21 S20speech-dispatcher -> ../init.d/speech-dispatcher
lrwxrwxrwx 1 root root  17 sep  9 23:08 S30vboxadd -> ../init.d/vboxadd
lrwxrwxrwx 1 root root  21 sep  9 23:10 S30vboxadd-x11 -> ../init.d/vboxadd-x11
lrwxrwxrwx 1 root root  25 sep  9 23:10 S35vboxadd-service -> ../init.d/vboxadd-service
lrwxrwxrwx 1 root root  15 sep  9 22:21 S50saned -> ../init.d/saned
lrwxrwxrwx 1 root root  19 sep  9 22:21 S70dns-clean -> ../init.d/dns-clean
lrwxrwxrwx 1 root root  18 sep  9 22:21 S70pppd-dns -> ../init.d/pppd-dns
lrwxrwxrwx 1 root root  21 sep  9 22:21 S99grub-common -> ../init.d/grub-common
lrwxrwxrwx 1 root root  18 sep  9 22:21 S99ondemand -> ../init.d/ondemand
lrwxrwxrwx 1 root root  18 sep  9 22:21 S99rc.local -> ../init.d/rc.local
```

També podrem posar en marxa o aturar el servei de forma manual, sense haver de reiniciar la màquina executant:

Arrencada:

`/etc/init.d/bind9 start`

Aturada:

`/etc/init.d/bind9 stop`

Podem verificar que ha arrencat correctament consultant el fitxer de registre 'syslog':

`tail -f /var/log/syslog`

reflectint a la sortida alguna cosa semblant a això:

```
root@servidor-primari:/etc/bind# /etc/init.d/bind9 stop
 * Stopping domain name service... bind9                                    [ OK ]
root@servidor-primari:/etc/bind# /etc/init.d/bind9 start
 * Starting domain name service... bind9                                    [ OK ]
root@servidor-primari:/etc/bind# tail -f /var/log/syslog
Sep 14 23:46:45 servidor-primari named[2551]: set up managed keys zone for view _default, file 'managed-keys.bind
'
Sep 14 23:46:45 servidor-primari named[2551]: command channel listening on 127.0.0.1#953
Sep 14 23:46:45 servidor-primari named[2551]: command channel listening on ::1#953
Sep 14 23:46:45 servidor-primari named[2551]: managed-keys-zone: loaded serial 3
Sep 14 23:46:45 servidor-primari named[2551]: zone 70.168.192.in-addr.arpa/IN: loaded serial 1
Sep 14 23:46:45 servidor-primari named[2551]: zone aulaSMX2.com/IN: loaded serial 1
Sep 14 23:46:45 servidor-primari named[2551]: all zones loaded
Sep 14 23:46:45 servidor-primari named[2551]: running
Sep 14 23:46:45 servidor-primari named[2551]: zone 70.168.192.in-addr.arpa/IN: sending notifies (serial 1)
Sep 14 23:46:45 servidor-primari named[2551]: zone aulaSMX2.com/IN: sending notifies (serial 1)
```

6.6. Configuració dels clients

Per defecte, els clients poden 'conèixer' els noms dels seus companys de la xarxa TCP/IP, **llegint la informació del fitxer hosts** situat a:

- Unix / Linux: **`/etc/`**
- Windows: **`c:\windows\system32\drivers\etc\`**

El **format d'aquest fitxer** és el mateix per a totes les plataformes, un exemple podria ser:

```
root@client:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       client
192.168.70.1    servidor-primari servidor-primari.aulaSMX2.com
```

L'inconvenient és que **caldria tenir-lo copiat** exactament igual **dins totes les màquines de la xarxa**.

Per evitar haver de distribuir i mantenir tots aquests fitxers tenim el servei de noms DNS, anem a veure com fer que els clients puguin utilitzar-lo.

6.6.1. Unix / Linux

Hem de fer client del servei DNS al mateix servidor, cal modificar dos fitxers:

- **`/etc/nsswitch.conf`**

  Cal verificiar l'existència de la línia:

  ```
  hosts:      files mdns4_minimal [NOTFOUND=return] dns mdns4
  ```

- **`/etc/resolv.conf`**

  Ha d'existir el següent contingut:

  ```
  search informaticaASIX2.com (o domain informaticaASIX2.com)
  nameserver 192.168.70.1
  ```

  Les dos línies següents no farien falta ja que les tenim als forwarders, per tant les podem esborrar.

  ```
  nameserver 192.168.202.2
  nameserver 8.8.8.8
  ```

Comprovem el correcte funcionament com a clients DNS executant:

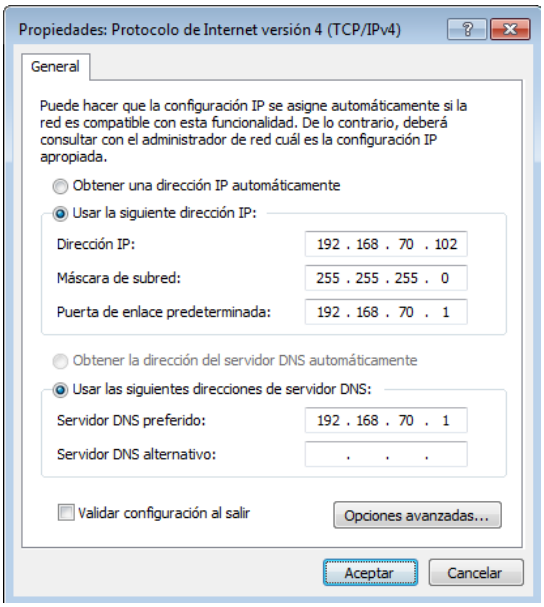
```
nslookup servidor-primari
```

obtenint com a resposta:

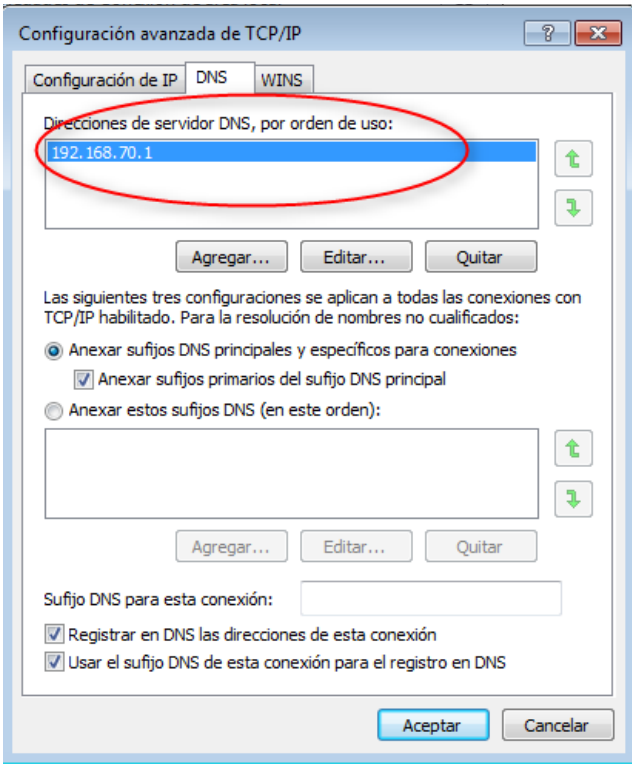
```
root@client:~# nslookup servidor-primari
Server:         192.168.70.1
Address:        192.168.70.1#53

Name:   servidor-primari.aulaSMX2.com
Address: 192.168.70.1
```

6.6.2. Windows

Modifiquem els paràmetres TCP/IP. En primer lloc configurem una IP dins del rang de la màquina servidor:



A les opcions avançades, modifiquem la configuració del DNS, dins les propietats de la xarxa, com mostra la figura:



Un cop reiniciat el Windows, podeu comprovar la resposta del DNS executant:

```
C:\Users\alumne>ping servidor-primari.aulaSMX2.com

Haciendo ping a servidor-primari.aulaSMX2.com [192.168.70.1] con 32 bytes de dat
os:
Respuesta desde 192.168.70.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.70.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ja teniu el servei DNS actiu dins la xarxa local, ara caldrà eliminar qualsevol referència dins els fitxers **hosts** (si els havíeu utilitzat), llevat del propi 'localhost' 127.0.0.1, per evitar definicions incorrectes que passarien pel davant del propi DNS.

6.7. Configuració DNS esclau

Si volem configurar el nostre servidor DNS per a que actuï com un esclau d'un servidor DNS mestre, la configuració és molt més simple que en el cas anterior ja que únicament serà necessari **indicar en el DNS esclau qui és el servidor DNS mestre**, **i en el DNS mestre, la IP del DNS esclau.**

Exemple, suposem que el nom del DNS mestre es servidor-primari.informaticaASIX2.com (IP 192.168.70.1) i que el nom del DNS esclau és servidor-secundari.informaticaASIX2.com. En l'arxiu 'db.ASIX2.hosts' de zona de cerca directa afegirem la línia del segon dns just baix del lloc on està la del primer:

```
// Afegir línia a /etc/bind/db.ASIX2.hosts del mestre
....
IN NS servidor-primari.informaticaASIX2.com.
IN NS servidor-secundari.informaticaASIX2.com. // Nova línia
....
```

d'aquesta forma indicarem que existeixen més servidors DNS per a una zona concreta. Farem el mateix a l'arxiu '192.168.70.rev' de la zona inversa:

```
// Afegir línea a /etc/bind/192.168.70.rev del mestre
....
IN NS servidor-primari.informaticaASIX2.com.
IN NS servidor-secundari.informaticaASIX2.com. // Nova línia
....
```

A l'arxiu /etc/bind/named.conf.local del servidor DNS esclau s'ha d'indicar que es tracta d'un servidor esclau i també s'ha d'indicar qui és el mestre:

```
// Afegir a /etc/bind/named.conf.local de l'esclau

zone "informaticaASIX2.com" {
      type slave;
      file "/etc/bind/db.ASIX2.hosts";
      masters { 192.168.70.1; };
      notify yes;
};
zone "70.168.192.in-addr.arpa" {
      type slave;
```

```
      file "/etc/bind/192.168.70.rev";
      masters { 192.168.70.1; };
      notify yes;
};
```

A l'arxiu /etc/bind/named.conf.local del servidor DNS mestre podem utilitzar la comanda also-notify per a mantenir els DNS sincronitzats. Amb also-notify passem els canvis de zones del mestre a l'esclau:

```
// Arxiu /etc/bind/named.conf.local del mestre

zone "informaticaASIX2.com" {
      type master;
      file "/etc/bind/db.ASIX2.hosts";
      also-notify {ip_de_l'esclau;};
      notify yes;
};
zone "70.168.192.in-addr.arpa" {
      type master;
      file "/etc/bind/192.168.70.rev";
      also-notify {ip_de_l'esclau;};
      notify yes;
};
```

D'aquesta forma **disposarem en la xarxa d'un servidor DNS esclau que podrà satisfer les peticions DNS a l'igual que ho faria el mestre**. És interessant si el número de peticions és molt elevat i es requereix distribuir la càrrega entre els dos servidors, o si desitgem disposar d'un servei DNS d'alta disponibilitat, **de forma que encara que el servidor mestre deixi de** funcionar, el servidor esclau podrà seguir oferint el servei.

Cada cop que féssim un canvi als arxius /etc/bind/db.ASIX2.hosts i /etc/bind/192.168.70.rev del mestre, hem de recordar-nos d'actualitzar el **paràmetre serial** (incrementar-lo en una unitat) per a que els dns dependents del mestre sàpiguen que ha canviat i actualitzin la seva informació i així mantenir-se perfectament sincronitzats.

6.7.1. Possibles errors en la configuració del DNS primari i DNS esclau

A continuació mostraré **alguns dels errors que ens podem trobar a mesura que anem configurant** els servidors DNS primari i secundari. La gran majoria de captures estan fetes al servidor secundari que és on ens trobarem els errors.

1. El primer que ens podem trobar és una **error en la connexió entre màquines** (host unreachable), això pot tenir diverses causes, però les més comuns són targetes mal configurades o fitxers de configuració del dns amb IPs mal introduïdes.

```
zone 70.168.192.in-addr.arpa/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
zone 70.168.192.in-addr.arpa/IN: Transfer started.
transfer of '70.168.192.in-addr.arpa/IN' from 192.169.70.1#53: failed to connect: host unreachable
transfer of '70.168.192.in-addr.arpa/IN' from 192.169.70.1#53: Transfer status: host unreachable
transfer of '70.168.192.in-addr.arpa/IN' from 192.169.70.1#53: Transfer completed: 0 messages, 0 records, 0 bytes, 2.521 secs (0 bytes/sec)
zone asix2.informatica.com/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
zone 69.168.192.in-addr.arpa/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
zone dam2.informatica.com/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
zone 168.192.in-addr.arpa/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
zone informatica.com/IN: refresh: retry limit for master 192.169.70.1#53 exceeded (source 0.0.0.0#0)
client 192.168.70.1#42484: received notify for zone 'dam2.informatica.com'
```

2. Un altre error típic és quan et diu que **no troba el fitxer o carpeta que li estàs indicant**, com es pot veure mostro el mateix cas un parell de cops, un per a la zona inversa de la xarxa (192.168.69.x) i un altra per a la zona directa (dam2.informatica.com). Fixem-nos que realment s'inicia la transferència i aparentment sembla que es realitza completament, però no és així.

```
zone 69.168.192.in-addr.arpa/IN: Transfer started.
transfer of '69.168.192.in-addr.arpa/IN' from 192.168.69.1#53: connected using 192.168.69.2#52203
zone 69.168.192.in-addr.arpa/IN: transferred serial 2
transfer of '69.168.192.in-addr.arpa/IN' from 192.168.69.1#53: Transfer status: success
transfer of '69.168.192.in-addr.arpa/IN' from 192.168.69.1#53: Transfer completed: 1 messages, 9 records, 292 bytes, 0.009 secs (32444 bytes/sec)
zone 69.168.192.in-addr.arpa/IN: sending notifies (serial 2)
dumping master file: /etc/bind/dam2/tmp-qElPLBL9ui: open: file not found
```

```
zone dam2.informatica.com/IN: transferred serial 2
transfer of 'dam2.informatica.com/IN' from 192.168.69.1#53: Transfer status: success
transfer of 'dam2.informatica.com/IN' from 192.168.69.1#53: Transfer completed: 1 messages, 10 records, 290 bytes, 0.008 secs (36250 bytes/sec)
zone dam2.informatica.com/IN: sending notifies (serial 2)
dumping master file: /etc/bind/dam2/tmp-LxlumJyHPs: open: file not found
```

3. Aquest error és semblant a l'anterior però en aquest cas ens dona **un error de 'permission denied'** i una altra informació sobre 'apparmor' que podem utilitzar per solucionar el problema.

```
Oct  4 10:12:25 servidor-secundari named[2788]: zone informatica.com/IN: transferred serial 2
Oct  4 10:12:25 servidor-secundari named[2788]: transfer of 'informatica.com/IN' from 192.168.70.1#53: Transfer status: success
Oct  4 10:12:25 servidor-secundari named[2788]: transfer of 'informatica.com/IN' from 192.168.70.1#53: Transfer completed: 1 messages, 13 records, 320 bytes, 0.036 secs (8888 bytes/sec)
Oct  4 10:12:25 servidor-secundari named[2788]: zone informatica.com/IN: sending notifies (serial 2)
Oct  4 10:12:25 servidor-secundari named[2788]: dumping master file: /etc/bind/tmp-M7poZKFz5F: open: permission denied
Oct  4 10:12:25 servidor-secundari kernel: [ 2432.410546] audit: type=1400 audit(1507104745.632:25): apparmor="DENIED" operation="mknod" profile="/usr/sbin/named" name="/etc/bind/tmp-M7poZKFz5F" p
id=2788 comm="named" requested_mask="c" denied_mask="c" fsuid=121 ouid=121
Oct  4 10:12:25 servidor-secundari kernel: [ 2432.411633] audit: type=1400 audit(1507104745.632:26): apparmor="DENIED" operation="mknod" profile="/usr/sbin/named" name="/etc/bind/tmp-hppIjy3pvJ" p
id=2788 comm="named" requested_mask="c" denied_mask="c" fsuid=121 ouid=121
```

6.7.2. Monitoritzant el bon funcionament del DNS de backup

Un cop tenim tots els errors solucionats, només ens queda **comprovar que la comunicació i transferència** d'informació entre servidors es realitza de forma correcta. La primera captura està feta al servidor principal, i es pot veure com **s'inicia i finalitza l'enviament** d'un parell de zones.

```
client 192.168.70.2#60431 (asix2.informatica.com): transfer of 'asix2.informatica.com/IN': AXFR started (serial 2)
client 192.168.70.2#60431 (asix2.informatica.com): transfer of 'asix2.informatica.com/IN': AXFR ended
client 192.168.69.2#45107 (69.168.192.in-addr.arpa): transfer of '69.168.192.in-addr.arpa/IN': AXFR started (serial 2)
client 192.168.69.2#45107 (69.168.192.in-addr.arpa): transfer of '69.168.192.in-addr.arpa/IN': AXFR ended
```

La segona està feta al servidor secundari i podem comprovar com **s'inicia la transferència de la zona directa 'asix2.informatica.com' i finalitza sense cap problema**. A més, et mostra informació sobre la quantitat de dades enviades i temps que ha tardat.

```
zone asix2.informatica.com/IN: Transfer started.
transfer of 'asix2.informatica.com/IN' from 192.168.70.1#53: connected using 192.168.70.2#60431
zone asix2.informatica.com/IN: transferred serial 2
transfer of 'asix2.informatica.com/IN' from 192.168.70.1#53: Transfer status: success
transfer of 'asix2.informatica.com/IN' from 192.168.70.1#53: Transfer completed: 1 messages, 10 records, 291 bytes, 0.004 secs (72750 bytes/sec)
zone asix2.informatica.com/IN: sending notifies (serial 2)
```

RECORDATORI - Comandes vàries per comprovar el funcionament del DNS:

- ***dig nom_de_la_zona*** ;comprovem que la zona està carregada correctament.
- **host direcció_IP_servidor_DNS** ;comprovem funcionament de la zona inversa.
- ***host nom_servidor_DNS*** ;comprovem funcionament de la zona directa.
- ***ping al DNS*** ;comprovem la comunicació amb el DNS.