Serveis de noms i de configuració automàtica

Eduard Canet i Ricart

Índex

Introducció

En el mòdul *Serveis de xarxa i Internet* estudiarem i practicarem la instal·lació i configuració de diversos serveis de xarxa. Molts d'aquests serveis són molt coneguts i són destinats a proporcionar serveis d'Internet a l'usuari final (per això són populars). Parlem per exemple del servei web (HTTP), el de transferència de fitxers (FTP), el de correu, el d'àudio, de vídeo... Tanmateix, hi ha altres serveis que tot i ser imprescindibles a Internet són menys coneguts per als usuaris. Es tracta de serveis com DHCP, DNS, SMTP..., que, tot i ser omnipresents, no són tan coneguts perquè no van destinats a l'usuari final, sinó a la configuració de les xarxes, a fer que les xarxes funcionin correctament.

En la unitat formativa **"Instal·lació i administració de serveis de noms de domini"** s'explica com mantenir i administrar adequadament els equips en xarxa de manera automatitzada. Es mostra com l'administrador pot establir serveis que permeten configurar automàticament les dades de connexió dels equips i el domini al qual pertanyen i com es configuren els equips per actuar de clients i fer ús d'aquests serveis.

En la unitat **"Instal·lació i administració de serveis de configuració automàtica de xarxa"** s'explica el protocol DNS (Domain Name System o sistema de noms de domini), que permet la resolució de noms de domini a adreces IP i a la inversa. La "màgia" amb la qual un usuari indica un nom de domini i obté l'adreça corresponent a aquest domini és obra del DNS.

Primerament caldrà que ens familiaritzem amb el sistema de noms de domini veient-ne l'evolució des dels primers fitxers de noms plans fins a l'actual sistema jeràrquic i distribuït. Aprendreu a reconèixer i a identificar el funcionament dels noms de domini a Internet i com són gestionats per mitjà de servidors encarregats de controlar una zona concreta.

Es presenta la documentació de l'estàndard del protocol DNS i les seves diverses extensions, que permeten actualitzacions dinàmiques, multitud d'opcions de configuració, configuracions condicionals, expressions i tractament de la seguretat en les comunicacions.

El sistema de noms de domini permet identificar un domini a qualsevol lloc del món a Internet. Es mostra com es realitza aquest mecanisme de resolució, que "per art de màgia" sap identificar quina adreça IP correspon a cada domini. Aquesta tasca la realitzen els servidors de noms. Cal, doncs, instal·lar-los i posar-los en funcionament. Veureu, doncs, tot el procés necessari per posar en marxa un servidor DNS i els mecanismes de reconeixement que cal utilitzar per comprovar-ne el funcionament correcte.

Finalment cal saber definir noves zones amb informació dels equips propis de la zona. S'explicarà com definir els equips usant els registres de recurs,

com compartir aquesta informació entre diversos servidors primaris i secundaris mitjançant transferències, com delegar zones entre institucions diferents i, fins i tot, com posar en marxa servidors només cau (que no administren res, simplement agiliten les respostes).

En l'apartat "Administra serveis de configuració automàtica, identificant-los i verificant la correcta assignació dels paràmetres" s'explica el funcionament del protocol DHCP. El servei DHCP (Dynamic Host Configuration Protocol o protocol de configuració dinàmica d'equips) permet la configuració d'adreces IP, màscares, passarel·les per defecte i moltes altres opcions de configuració de manera totalment dinàmica. A cada equip, se li ha de proporcionar un identificador i la informació necessària per poder treballar en xarxa i poder accedir a altres equips i altres xarxes.

Primerament analitzem quina és la informació que ha de tenir un equip per poder treballar en xarxa i disposar d'accés a Internet. Aquesta configuració es pot establir manualment o de manera dinàmica; s'analitzen els pros i contres de cada cas. El creixement que han sofert les xarxes a escala mundial (tant en nombre de xarxes com d'equips i de complexitat de gestió) va propiciar el sorgiment del protocol DHCP. Se n'estudia l'origen, basat en el protocol BOOTP, l'evolució i el funcionament. Així, doncs, descriurem el clàssic diàleg DHCP d'intercanvi de quatre missatges.

Un cop es coneix la finalitat del protocol DHCP i el seu funcionament, cal implementar-ne un servidor. Estudiarem tots els passos necessaris per fer-ho i tots els mecanismes de reconeixement i monitoratge per comprovar que la instal·lació i posada en servei s'han fet correctament.

Finalment cal estudiar les opcions de configuració generals del servei i fer un repàs a les opcions de xarxa més usuals per als clients.

També veurem la configuració d'un client DHCP i les opcions que es poden definir directament en el client.

Els dos temes tractats en aquesta unitat, tot i que relacionats, són absolutament independents l'un de l'altre. Us recomanem fer una primera lectura global del servei DNS i en una segona lectura anar practicant in situ en un servidor els passos que es van descrivint. Aquest procés pràctic es pot ampliar al mateix temps seguint els apunts i les activitats contingudes en el material web. El mateix procediment es pot aplicar per aprendre el funcionament del servei DHCP i per practicar la configuració d'un servidor.

Resultats d'aprenentatge

En acabar aquesta unitat, l'alumne:

1. Administra serveis de resolució de noms, analitzant-los i garantint la seguretat del servei.

- Identifica i descriu escenaris en els quals sorgeix la necessitat d'un servei de resolució de noms.
- Classifica els principals mecanismes de resolució de noms.
- Descriu l'estructura, la nomenclatura i la funcionalitat dels sistemes de noms jeràrquics.
- Instal·la i configura serveis jeràrquics de resolució de noms.
- Prepara el servei per reexpedir consultes de recursos externs a un altre servidor de noms.
- Prepara el servei per emmagatzemar i distribuir les respostes procedents d'altres servidors.
- Afegeix registres de noms corresponents a una zona nova, amb opcions relatives a servidors de correu i àlies.
- Implementa solucions de servidors de noms en adreces IP dinàmiques.
- Realitza transferències de zona entre dos o més servidors.
- Documenta els procediments d'instal·lació i configuració.

2. Administra serveis de configuració automàtica, identificant-los i verificant la correcta assignació dels paràmetres.

- Reconeix els mecanismes automatitzats de configuració dels paràmetres de xarxa i els avantatges que proporcionen.
- Il·lustra els procediments i les pautes que intervenen en una sol·licitud de configuració dels paràmetres de xarxa.
- Instal·la servidors de configuració dels paràmetres de xarxa.
- Prepara el servei per assignar la configuració bàsica als equips d'una xarxa local.
- Configura assignacions estàtiques i dinàmiques.
- Integra en el servei opcions addicionals de configuració.
- Documenta els procediments realitzats.

1. Instal·lació i administració de serveis de noms de domini

El **sistema de noms de domini** o **DNS** (Domain Name System) proporciona un mecanisme eficaç per fer la resolució de noms de domini a adreces IP. Com a usuaris (humans) ens és més fàcil adreçar-nos a un nom de domini (de *host*, de web, de servidor de correu...) utilitzant un text identificatiu com per exemple www.ioc.cat que no pas l'adreça IP 213.73.40.230. El servei DNS no solament permet fer la resolució de noms de domini a adreces IP, sinó també la resolució inversa. És a dir, a partir d'una adreça IP esbrinar el nom de domini del *host*.

El servei DNS proporciona independència del nom de domini respecte a l'adreça IP. Així un domini pot canviar d'adreça IP de manera transparent per als usuaris del domini. Fins i tot és usual que un domini s'identifiqui amb més d'una adreça IP com a mesura de redundància contra la caiguda del sistema o com a balanceig de càrregues. Altres serveis proporcionats pel DNS són la identificació dels servidors de correu d'un domini, de cada un dels *hosts* que pertanyen a la xarxa, servidors d'impressió...

1.1 El servei de resolució de noms

El problema d'identificar els equips es produeix des de bon principi de l'existència de les xarxes d'ordinadors i no és específic de les xarxes TCP/IP. Cal un mecanisme en "llenguatge humà" per identificar els equips de la xarxa. En especial els que proporcionen serveis als altres equips i usuaris. En la xarxa inicial Arpanet, els equips ja rebien un nom. Aquests noms es feien públics per mitjà d'un fitxer centralitzat que contenia els noms de tots els equips de la xarxa i la seva identificació. Aquest fitxer era hosts.txt, conegut en sistemes GNU/Linux com a /etc/hosts.

> Un **sistema de noms pla** es basa en la utilització d'un **fitxer de text** que descriu cada *host* amb la seva corresponent adreça IP. Es pot usar per definir àlies per equips locals en xarxes petites, però no és escalable a xarxes grans, i molt menys a Internet.

En una xarxa petita es pot generar un fitxer amb el nom i l'adreça IP de tots els *hosts* centralitzat en un servidor, i encarregar-se de distribuir còpies d'aquest fitxer a tots els equips de la xarxa. Però aquest model de coneixement no és escalable. Si la xarxa creix és impossible de mantenir. Utilitzar aquest model significaria que hi ha un equip que centralitza els noms de tots els *hosts* d'Internet en un sol fitxer! D'altra banda, també significaria que aquest fitxer s'ha de repartir entre tots els equips d'Internet perquè sàpiguen com es diuen els altres equips cada cop que hi ha una actualització. Evidentment cal una altra solució.

El 1983 sorgeix el Domain Name System (DNS) per aportar una solució escalable i pràctica. El DNS es fonamenta en una base de dades de noms de domini jeràrquica i distribuïda. És **jeràrquica** perquè s'organitza en una estructura de **dominis** que es poden compondre de subdominis que també es poden dividir en subdominis i així fins a 127 nivells (originàriament). Aquests dominis són gestionats per servidors DNS responsables de cada **zona**. I és una base de dades **distribuïda** perquè la informació no està tota junta en un sol repositori central, sinó que es troba repartida per parts en els servidors DNS d'Internet. Cada servidor DNS **autoritari** conté la base de dades de la seva zona.

1.1.1 Classificació dels mecanismes de resolució

Els administradors de xarxes tenen la tasca d'establir el mecanisme d'identificació de *hosts* que volen usar. Determinar quins noms usaran i com es farà per identificar cada nom amb l'adreça IP corresponent. Els mecanismes per anomenar els *hosts* pot ser local a cada *host*, local i intern a una organització i global a Internet.

Un cop posats els noms cal saber-los resoldre, trobar-ne l'adreça IP apropiada. La resolució pot ser local en un *host* usant un fitxer d'associacions o implementada usant el servei de noms DNS. Aquest servei es basa en l'estructura client/servidor, de manera que caldrà aprendre a configurar tant l'un com l'altre. Primerament es descriurà com configurar el client o *resolver* i el servidor serà tractat al llarg dels apartats posteriors. Aquests dos mecanismes, local i DNS, es poden combinar i determinar-ne la precedència.

El servei DNS proporciona múltiples maneres de treballar. Segons quina sigui la seva configuració actuarà de manera diferent en fer la resolució. Caldrà estudiar què és un servidor només cau, què fa quan es permet la utilització de la memòria cau, la utilització d'un forwarder i quina diferència hi ha entre usar recursió o no utilitzar-la. La gestió de dominis i zones pròpies, la creació de subdominis i la delegació són aspectes clau del funcionament d'un servidor de noms de domini que també es tractaran més endavant.

1.1.2 Noms de 'host' locals, dominis locals i dominis d'Internet

Sabem que els *hosts* s'identifiquen en una xarxa i a Internet per la seva adreça IP, però en general els usuaris desconeixen quina és aquesta adreça. Els usuaris estan habituats a connectar-se per exemple a un altre dels ordinadors de casa seva posant un *nom local* que s'han inventat (per exemple, pcJocs, portatilMarta...).

A la feina, els mateixos usuaris accedeixen a diversos equips que tenen noms que els hi han posat els administradors del sistema. Així, per exemple, els informes estan en un ordinador anomenat *watergate*, la gestió de la comptabilitat en un

servidor que es diu *blackhole* i les nòmines es gestionen des del servidor *minix*. Tots aquests ordinadors pertanyen a la xarxa de l'empresa, que s'identifica amb el nom de domini local empresa.cat.

A més a més, resulta que tant des de casa com des de la feina aquests usuaris treballen habitualment consultant serveis a *hosts* com gmail.com, youtube.com, ara.cat... És a dir, consulten serveis i *hosts* de dominis d'Internet.

Aquests tres casos exposats permeten observar tres tipus diferents de resolució de noms:

- Resolució de noms de *host* locals
- Resolució de noms d'un domini local (no integrat a Internet)
- Resolució de noms global (domini integrat a Internet)

Les tres resolucions no són excloents, sinó que s'implementen totes a la vegada combinant la resolució local i la resolució via DNS. Existeix també un mecanisme per indicar la precedència de la resolució, és a dir, indicar si es prefereix primer la resolució local i després la de DNS o a l'inrevés.

1.1.3 El client DNS: 'resolver'

Un equip client que vol resoldre un nom de *host* té diferents maneres de fer-ho. Es pot fer localment mitjançant un fitxer de *hosts* (típicament /etc/hosts) o de manera distribuïda usant DNS (el *resolver*). De fet, es poden aplicar tots dos mètodes conjuntament indicant-ne la precedència en algun fitxer de configuració del sistema (en sistemes GNU/Linux, el fitxer /etc/ nsswitch.conf).

El *resolver* és la part client del sistema de noms de dominis DNS, que està organitzat en una estructura client/servidor. Cada *resolver* implementa les seves opcions, però n'hi ha que són suficientment genèriques per descriure-les aquí. En la majoria de sistemes GNU/Linux, aquestes opcions es defineixen en el fitxer /etc/resolv.conf.

Criteri de resolució

Per defecte, quan cal resoldre un nom de *host* (i no s'ha especificat la directiva *search*), el *resolver* fa el següent: si el nom de *host* inclou un punt (pc30.inf) mira de resoldre'l tal qual, i si no pot hi aplica el nom de domini (pc30.inf.inf.fpoberta.net.). Si el nom de *host* no conté cap punt (pc30), primer li afegeix el domini i el mira de resoldre (pc30.inf.fpoberta.net.), i si no el troba el mira de resoldre tal qual (pc30).

Les següents són les directives del fitxer /etc/resolv.conf:

- **domain** (*local domain name* o nom de domini local) indica el nom de domini del *host* al qual pertany el *resolver*. Serveix per completar els noms de domini no qualificats (FQDN).

- **search** permet modificar el comportament per defecte indicant explícitament la llista de dominis a aplicar. El primer d'aquests és aplicat com el nom del domini local (*local domain name*) i és per això que la directiva *search* és excloent de la directiva *domain*.

- **nameserver** permet especificar el servidor de noms a utilitzar. Se'n poden indicar fins a tres per si no hi ha accés al servidor. El *resolver* intenta connectar amb el primer servidor i si ho aconsegueix realitza les consultes a aquest servidor.

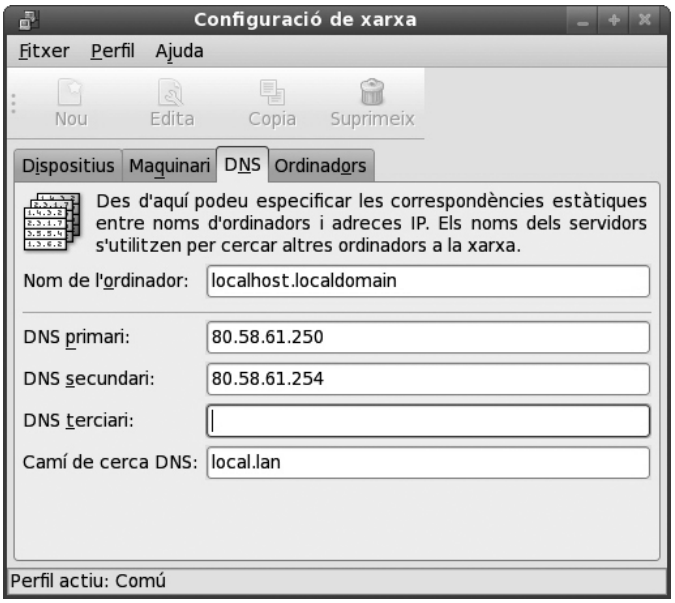
Servidor de noms d'una altra organització

Es poden configurar els *hosts* perquè utilitzin el servidor de noms d'una altra organització (perquè és més ràpida, per estalviar-se feina...), però no és una bona pràctica.

```
# Exemple de fitxer de configuració client /etc/resolv.conf
[root@host ~]$ cat /etc/resolv.conf
search ioc.cat
nameserver 80.58.61.250
nameserver 80.58.61.254
```

La figura 1.1 mostra una interfície gràfica que permet configurar els servidors DNS. En aquest exemple s'observa que s'han definit dos servidors de noms, un de primari i un de secundari. La directiva *search* correspon al valor local.lan. Tal com és habitual en sistemes GNU/Linux aquesta miniaplicació gràfica (*applet*) simplement modifica el fitxer de configuració.

FIGURA 1.1. Miniaplicació gràfica de configuració del resolver



1.2 Funcionalitat del sistema de noms jeràrquics

Sabem que tenim la necessitat de poder-nos adreçar als diversos *hosts*, servidors i dominis que hi ha a les xarxes, i en especial a Internet. Hem d'establir algun mètode per relacionar les adreces IP amb el seu nom corresponent. Un mecanisme és posar noms plans als *hosts* i als dominis, noms independents els uns dels altres sense cap mena d'estructura ni de jerarquia. Amb tota seguretat aquest mecanisme provocaria noms duplicats i un caos organitzatiu important.

El sistema de noms de domini permet identificar qualsevol equip en la xarxa i assegurar-se que no hi ha col·lisions, és a dir, noms duplicats. Es basa en una estructura jeràrquica de noms en forma d'arbre on l'arrel és el node o domini arrel del qual deriven tots els altres nodes. Aquest es divideix en altres dominis com, per exemple, .com, .edu, .org, .cat... Al seu torn, cada domini es pot dividir en

subdominis i així successivament. Les rutes s'indiquen començant pel subdomini més intern i anant cap al node arrel, com per exemple mail.ioc.cat.

1.2.1 El sistema de noms jeràrquic

En un sistema de noms jeràrquic cada node de l'arbre s'identifica per un text (el nom de domini) que no es pot repetir en el mateix nivell, però sí en altres llocs de l'arbre de l'espai de noms. El mateix passa amb els fitxers: no hi pot haver dos fitxers amb el mateix nom en el mateix directori, però sí en ubicacions diferents. Un **domini** està format pel propi node i la resta de l'arbre que penja d'aquest node. Penseu en l'exemple d'un directori: si es vol copiar un directori s'entén que està format pel mateix directori i tots els subdirectoris que conté.

Caràcters en els noms de domini

L'estàndard DNS indica que els noms de domini han de ser de 64 caràcters com a màxim, i només poden incloure caràcters llatins, dígits del 0 al 9 i el guió. Les majúscules són indiferents.

Hi ha mecanismes com l'IDNA (Internationalized Domain Name o noms de domini internacionalitzats) que permeten utilitzar altres alfabets en els noms de domini.

Anomenem **espai de noms** al conjunt de tots els dominis que formen l'arbre de noms DNS. Continuant l'analogia amb el sistema de fitxers diríem que l'espai de noms és equivalent a tot el sistema de fitxers i directoris.

El sistema de noms de domini d'Internet DNS està format pels elements següents:

- **Espai de noms**: el conjunt de tots els noms de domini d'Internet (tot l'arbre).
- **Domini**: text identificatiu d'un domini (un node i tots els seus descendents).
- **FQDN**: nom de domini absolut començant pel node i acabant en l'arrel.
- **Domini absolut**: és un sinònim d'FQDN. Es la ruta sencera que va del node a l'arrel. Els dominis absoluts acaben en punt.
- **Domini relatiu**: nom de domini sense qualificar (no acaba en punt). S'entén que un nom de domini és relatiu al domini al que pertany.
- **Domini arrel**: domini del qual deriven tots els altres. S'indica amb un punt o amb la cadena buida.

Exemples de noms de domini:

El punt final en els noms de domini

La majoria de vegades escrivim els dominis com si fossin absoluts, però són relatius al node arrel perquè no posem el punt final. Un altre cop es pot fer l'analogia amb les rutes relatives i les rutes absolutes del sistema de fitxers.

- ioc.cat.: nom de domini absolut que, per exemple, inclou mail.ioc.cat i inf.ioc.cat.
- pc01.inf.ioc.cat.: nom de *host* absolut o FQDN.
- pc01: nom de *host* relatiu al domini on pertanyi.
- pc02.inf: nom de domini relatiu al domini on pertany.
- com: nom de domini relatiu. Usualment ens hi referim en lloc de com., que és el FQDN apropiat.
- .: domini arrel.

L'estructura d'arbre (jeràrquica) de l'espai de noms proporciona un mecanisme d'identificació únic d'un domini. No pot existir cap domini que tingui exactament el mateix nom absolut o **FQDN** (Fully Qualified Domain Name o nom de domini complet). Els dominis es llegeixen des del node a l'arrel. Així, un domini que correspongui al departament d'administració de l'organització IOC dins del domini cat s'identifica, per exemple, com a admin.ioc.cat. Si ens fixem en el domini anterior, veurem que acaba en punt: és una manera d'indicar el domini arrel. El **domini arrel** es defineix com un domini sense etiqueta o, millor dit, amb la cadena buida com a etiqueta. Això provoca que els dominis que s'indiquin de manera absoluta acabin amb el caràcter punt.

Un **domini absolut** o FQDN és el que inclou tots els nodes des del domini fins a l'arrel (inclosa en forma de punt final). Un **domini relatiu** no inclou l'arrel i pot ser relatiu al domini actual. Per exemple, dins del domini de l'IOC el domini inf (del departament d'informàtica) és un nom relatiu que fa referència al nom absolut inf.ioc.cat.

1.2.2 Els noms de domini d'Internet

Origen dels noms de domini

Si ens fixem en els primers dominis d'alt nivell, estaven basats en una visió estatunidenca del món (de fet la xarxa Arpanet, base de l'actual Internet, va ser desenvolupada pel Departament de Defensa del govern dels EUA). En estendre's Internet globalment i aparèixer dominis d'alt nivell geogràfics, moltes organitzacions es van registrar en més d'un domini (per exemple, empresa.com i empresa.cat).

A Internet els noms de dominis segueixen una estructura basada en els seus inicis però que ha anat evolucionant. El node arrel es va dividir en un conjunt de subdominis anomenats **TLD** (Top Level Domains o dominis d'alt nivell). Aquests dominis eren com, edu, gov, mil, org, net i int. Posteriorment se'n van afegir d'altres com cat, name, biz, info, pro, aero, coop i museum. Es volien organitzar els dominis per funcionalitat posant les empreses en els .com, les organitzacions en els .org...

Es va veure, però, la necessitat de poder agrupar els dominis de manera geogràfica i van sorgit els famosos identificadors de país. Per a cada país es va generar un TLD de dos caràcters utilitzant el preexistent estàndard internacional ISO 3166 (els famosos .es, .fr, .us...).

Degut a aquesta doble nomenclatura, els primers es coneixen com **gTLD** (domini de primer nivell genèric, en anglès *generic top-level domain*) i els segons corresponents a països com a **ccTLD** (domini de primer nivell territorial, en anglès *country-code top-level domain*).

Els servidors arrel són crucials per al funcionament del DNS, ja que coneixen tots els dominis de primer nivell. Han d'admetre un gran volum de consultes i per això n'hi ha tretze repartits per tot el món. A més a més, d'aquests tretze, alguns tenen rèpliques en diversos continents utilitzant un sistema anomenat *anycast*.

Dominis d'alt nivell

Els següents són exemples de dominis d'alt nivell:

- cat: Catalunya
- ad: Andorra

- aq: Antàrtida
- gb: Gran Bretanya
- im: Illa de Man
- ms: Montserrat
- pf: Polinèsia Francesa
- ps: autoritat palestina
- uk: Regne Unit

Així doncs, hi ha un node arrel del qual deriven múltiples nodes de primer nivell, com per exemple com., cat., es., org. Aquests dominis són gestionats per institucions o empreses amb forts lligams amb la indústria informàtica i Internet. Després hi ha els dominis de segon nivell, com per exemple ioc.cat., gmail.com., rediris.es. o escoladeltreball.org., que corresponen a empreses o institucions que han demanat disposar d'un domini propi de segon nivell. Això es fa demanant donar-se d'alta al gestor apropiat del domini de primer nivell del qual es vol formar part. Aquests serveis són de pagament en la gran majoria dels casos.

El model es va repetint de manera que cada gestor d'un domini pot crear (o vendre) subdominis del seu domini. Així, per exemple, si els gestors del domini imaginari *jocs.org.* permeten fer subdominis, es podria crear el subdomini *parxis.jocs.org.* des d'on divulgar la nostra afició al parxís.

A vegades els dominis es classifiquen per nivells, indicant el seu grau de profunditat:

- **Arrel**: el domini pare de tots els dominis, el punt.
- **TLD** o **primer nivell**: domini fill de l'arrel o de primer nivell. En són exemples cat., es., com., org. ...
- **Segon nivell**: format pels dominis fills dels dominis de primer nivell. Per exemple, ioc.cat., gencat.cat., gmail.com., python.org. ...
- **Altres**: a partir d'aquí cada domini de segon nivell genera els subdominis que creu apropiats. Alguns són gestionats per ells mateixos i d'altres són delegats a altres entitats. Per exemple, correu.ioc.cat., ensenyament.gencat.cat.

Els dominis inclouen *hosts*, impressores, servidors de correu... És a dir, noms d'una màquina. Tot nom de *host* és també un nom que es podrà identificar i resoldre usant el DNS. Els noms de *host* pertanyen a un domini, però no són dominis. Sovint els usuaris desconeixen la diferència entre un nom de *host* (un element) i un nom de domini (una àrea que abasta subdominis i que conté *hosts*). Veurem més endavant la relació entre els dominis i les zones, que són les bases de dades que descriuen els *hosts* que formen part del domini.

Per exemple, gmail.com. és un domini, però www.gmail.com. és un *host* (o més d'un en cas de ser *multihomed*). El mateix passa amb inf.ioc.cat., que fa referència al domini format per tots els *hosts* del departament d'informàtica de l'IOC i els possibles subdominis que tingui. En canvi, pc01.inf.ioc.cat., printer.inf.ioc.cat. o ftp.inf.ioc.cat. són noms de *hosts* que pertanyen a aquest domini.

Molt sovint a Internet es confon entre un **nom de *host*** com ftp.rediris.es., que identifica la màquina de RedIRIS que proporciona el servei FTP, i el **nom de domini**, que identifica una àrea de l'espai de noms de domini que inclou els seus subdominis.
Els **dominis** contenen descripcions dels *hosts* i la seva organització.

Alguns exemples són:

- www.gmail.com. és un nom de *host*.
- gmail.com. és un nom de domini.
- www.ioc.cat. és un nom de *host*.
- ioc.cat. és un nom de domini.

```
# Llistat de l'adreça IP d'un host concret ("eines") del domini ioc.cat
root@server:~# host eines.ioc.cat
eines.ioc.cat has address 85.192.111.246

# Llistat d'informació global del domini ioc.cat
root@server:~# host ioc.cat
ioc.cat has address 85.192.111.254
ioc.cat mail is handled by 10 aspmx.l.google.com.
ioc.cat mail is handled by 20 alt2.aspmx.l.google.com.
ioc.cat mail is handled by 30 aspmx4.googlemail.com.
ioc.cat mail is handled by 30 aspmx5.googlemail.com.
ioc.cat mail is handled by 20 alt1.aspmx.l.google.com.
ioc.cat mail is handled by 30 aspmx3.googlemail.com.
ioc.cat mail is handled by 30 aspmx2.googlemail.com.
```

1.2.3 Dominis, subdominis i zones

Exemple d'administració de subdomini

El domini .cat és administrat per una entitat que gestiona la zona .cat. Aquest domini conté el subdomini ioc.cat, però ha **delegat** l'administració d'aquest subdomini a l'IOC. Els administradors de l'IOC disposen d'un servidor que gestiona el seu domini com una zona. El domini .cat és l'arbre que inclou tots els dominis que en deriven, inclòs ioc.cat. Però la zona .cat i la zona ioc.cat no són la mateixa zona. Són administrades per entitats diferents.

Sabem que el sistema de noms de domini està basat en una arquitectura client/servidor en què els clients fan preguntes del tipus "Quina IP té aquest domini?" i els servidors miren de contestar-les. Els servidors de noms DNS són els programes que emmagatzemen i gestionen la informació de la base de dades d'una part de l'espai de noms anomenada *zona*.

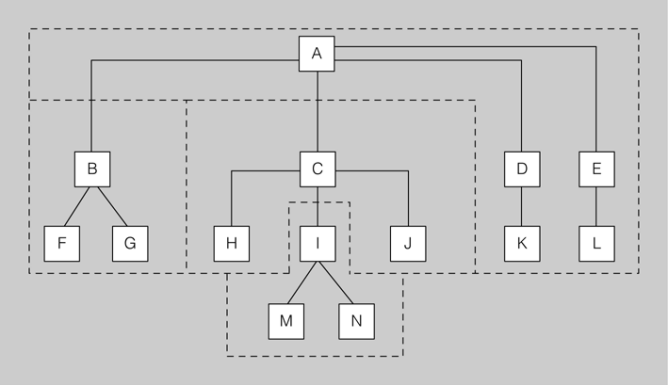
Primerament hem de descriure què és una zona. Una **zona** és la part de l'espai de noms de domini gestionada per un o més servidors DNS. Els servidors que gestionen la zona tenen informació completa sobre ella i es diu que hi tenen **autoritat**. Podríem pensar que un servidor DNS gestiona un domini i que una zona és el mateix que un domini, però això no és necessàriament així. Un domini

es divideix en subdominis per facilitar-ne l'administració. Cada part administrada per un o més servidors DNS és una zona. El domini és l'arbre de l'espai de noms (ell i els seus descendents) i la zona és la part de l'arbre administrada per un servidor de noms de domini concret.

En la figura 1.2 es pot veure un espai de noms amb quatre zones i catorze dominis. Cada lletra és un domini. El nom de domini corresponent a cada zona (s'anomenen segons el seu node superior) és A, B.A, C.A i I.C.A respectivament. Cada una d'aquestes quatre zones tindrà un o més servidors DNS per gestionar-la.

En general, podem dir que una zona conté la informació completa dels equips que formen el domini corresponent a la zona i dels equips dels subdominis que no s'han delegat. Aquesta informació s'emmagatzema en la **base de dades de zona**.

Figura 1.2. Exemple de zones i dominis



Convé tenir clar en tot moment que domini i zona no són equivalents (tot i que poden coincidir).

- El **domini** és l'arbre de l'espai de noms que inclou el node i els seus descendents.
- La **zona** és la part de l'arbre administrada per un servidor DNS concret.
- La **base de dades de zona** la formen els fitxers que emmagatzemen la descripció dels equips que pertanyen a la zona.
- La **delegació** consisteix a passar l'autoritat de la gestió d'un subdomini a una altra entitat. Aquesta serà qui s'encarregarà de gestionar-lo.

Delegar l'administració d'un subdomini no és més que traspassar l'autoritat sobre aquest subdomini a una altra entitat (a uns altres servidors DNS). Aquesta entitat és la responsable de l'administració de la zona delegada. Té tota l'autoritat per fer i desfer al seu criteri. La zona pare perd el control administratiu de la zona delegada i simplement apunta als servidors de noms de la zona delegada per obtenir informació quan la requereix.

L'estàndard que defineix el DNS estableix que cal configurar dos o més servidors autoritaris per a cada zona, anomenats *servidor primari* i *servidor secundari*. El motiu és proporcionar un mecanisme de redundància, robustesa, rendiment i còpia de seguretat. Si el servidor de noms falla i és únic, possiblement la xarxa caurà, serà inoperativa.

Els servidors **primari** (o *master*) i **secundari/s** (o *slave/s*) són autoritat. Només el primari té els fitxers de zona amb les dades in situ. Els servidors secundaris obtenen una còpia de les dades per transferència.

1.2.4 El protocol DNS

El servei de noms de domini utilitza el protocol DNS per fer les consultes i les respostes. Es tracta d'un protocol de capa d'aplicació que pot utilitzar tant UDP (*User Datagram Protocol*) com TCP (*Transmission Control Protocol*) en la capa de transport. Usualment, tant les consultes del client com les respostes del servidor es poden encabir en un datagrama (512 *bytes*) i s'utilitza UDP (de fet, generalment es diu que el DNS usa UDP). Però si la informació a transmetre és àmplia (per exemple, una resposta amb una llista amb molta informació), la comunicació es passa automàticament a TCP. Un altre cas en què la informació usa TCP és quan es realitza la transferència d'informació d'una zona entre servidors primaris i secundaris. El servidor DNS utilitza el port ben conegut (*well known*) 53.

El **protocol DNS** usu habitualment UDP, però pot usar **TCP i UDP**. Es tracta d'un protocol de capa d'aplicació i utilitza el **port 53**.

Els datagrames DNS es componen de diversos apartats, tal com es pot veure en la consulta *host* següent:

```
root@server:~# host -a uoc.edu
Trying "uoc.edu"
Trying "uoc.edu"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39287
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
uoc.edu.    3600  IN  TXT "google-site-verification=
    GrOoO_KKCaNNqkn4y6c3P_AnaoSczfz_mKBeSo4DKZ8"
uoc.edu.    3600  IN  TXT "google-site-verification=
    GxX8kwaNhmRhDUaZrmgdOALPvdor5iFnIorJBGYcEcw"
uoc.edu.    3600  IN  TXT "v=spf1 ip4:213.73.40.0/24 ip4:13.111.22.169 ip4
    :83.169.91.142 ip4:83.169.91.143 ip4:83.169.91.144 ip4:83.169.91.145 ip4
    :83.169.91.146 ip4:83.169.91.147 include:_spf.google.com include:eevid.com
     ~all"
uoc.edu.    3600  IN  TXT "adobe-idp-site-verification=f6f2f671-9e0b
    -4464-9293-5c71951acbc1"
uoc.edu.    86400 IN  NS  nepal.uoc.es.
uoc.edu.    86400 IN  NS  tibet.uoc.es.
```

```
17 uoc.edu.    86400 IN  SOA tibet.uoc.es. root.tibet.uoc.es. 2020063001 286400
       7200 2592000 172800
18 uoc.edu.    600 IN  A 213.73.40.242
19 uoc.edu.    300 IN  NAPTR 0 30 "S" "SIP+D2U" "" _sip\._udp\.uoc\.edu.
20 uoc.edu.    300 IN  MX  5 alt2.aspmx.l.google.com.
21 uoc.edu.    300 IN  MX  10 aspmx2.googlemail.com.
22 uoc.edu.    300 IN  MX  10 aspmx3.googlemail.com.
23 uoc.edu.    300 IN  MX  10 aspmx4.googlemail.com.
24 uoc.edu.    300 IN  MX  10 aspmx5.googlemail.com.
25 uoc.edu.    300 IN  MX  1 aspmx.l.google.com.
26 uoc.edu.    300 IN  MX  5 alt1.aspmx.l.google.com.
27
28 ;; ADDITIONAL SECTION:
29 tibet.uoc.es.   86291 IN  A 213.73.40.45
30
31 Received 819 bytes from 192.168.1.1#53 in 6438 ms
```

La comunicació DNS és un mecanisme de consulta/resposta entre el client i el servidor. Els datagrames, doncs, seran de *query* (consulta) o *answer* (resposta).

Els apartats que componen un missatge DNS són:

- **HEADER**. Capçalera del missatge que indica si és una consulta o una resposta. Conté l'ID (identificador) del missatge, *flags* i un resum de quines seccions del missatge porten informació i quanta.
- **QUESTION**. Aquesta secció conté la consulta que s'ha efectuat. És a dir, quina dada s'ha demanat al servidor. Pot ser una resolució d'adreça IP a un domini, demanar la llista de servidors de correu...
- **ANSWER**. Secció que conté la resposta obtinguda del servidor. S'entén que aquesta secció conté la resposta no autoritativa. A vegades en les utilitats de consulta aquesta secció es mostra com a *non-authority answer*.
- **AUTHORITY**. Aquesta secció conté les respostes que són autoritatives per a la consulta efectuada. Evidentment pot estar buida.
- **ADDITIONAL**. Conté informació addicional per completar la resposta. En l'exemple s'observa que completa la resolució dels noms de màquina que hi ha a la secció *answer* tot indicant la seva adreça IP corresponent.

1.3 Instal·lació i configuració del servei DNS

El servei de xarxa DNS està estructurat en forma de servei client/servidor; per tant, caldrà disposar del programari apropiat per adoptar cada un d'aquests rols. El programari que fa la funció de client usualment ja està integrat en el sistema operatiu (la part que gestiona la xarxa) o en les mateixes aplicacions (per exemple, Firefox). És a dir, per disposar de la part client del servei DNS normalment no cal instal·lar res, tot i que sí que cal configurar-la correctament.

Així, doncs, quan parlem d'instal·lar un servei DNS fem referència al procés d'instal·lació i configuració del programari del servidor.

La instal·lació del programari que proporciona el servei DNS es fa de manera molt similar (per no dir idèntica) a la d'altres serveis de xarxa com el DHCP, l'HTTP o l'FTP. Es tracta d'instal·lar el programari de l'aplicació servidor i fer-ne la configuració apropiada.

Per fer tot això cal fer les reflexions i passos següents:

- Quin programari proporciona aquest servei? Quines característiques té? Com es pot adquirir?
- Obtenir l'aplicació que proporciona el servei DNS.
- Observar l'estat de la xarxa actual. Està el servei ja en funcionament? Existeix ja una configuració DNS activa?
- Instal·lar l'aplicació servidor.
- Comprovar que la instal·lació s'ha efectuat correctament.
- Configurar el servei en el servidor i activar els clients perquè la utilitzin.
- Comprovar que el servei funciona correctament.

1.3.1 Aplicacions servidor DNS

Sempre que l'administrador vol posar en funcionament un nou servei de xarxa cal que primerament analitzi quines aplicacions hi ha en el mercat que ofereixen aquest servei. És feina seva estudiar les característiques de les diverses aplicacions, com per exemple avaluar-ne l'eficiència, el cost, el que en diuen els altres... La manera més fàcil de fer això és navegar per Internet, consultar les revistes especialitzades o demanar consell a un dels gurus informàtics coneguts.

Cerca de DNS a Internet

Usualment l'administrador s'informa mitjançant el seu cercador preferit, per exemple Google, i de webs com la Viquipèdia. Proveu a buscar "DNS" o "DNS server" al Google i a la Wikipedia (en anglès).

Usualment, però, l'administrador acaba utilitzant l'aplicació servidor DNS que li proporciona el mateix sistema operatiu. Si utilitzeu Windows, l'empresa Microsoft disposa d'una aplicació pròpia, però també en podeu trobar d'altres a Internet. Igualment, si utilitzeu GNU/Linux, segurament la mateixa distribució ja proporciona un servidor DNS o bé n'existeix algun de clàssic provinent de l'Unix. De totes maneres, també en podeu obtenir d'altres a Internet. En la figura 1.3 es pot veure quin servidor utilitzen els nodes arrels. La llista ha estat extreta de la Wikipedia. S'hi poden observar els 13 servidors o nodes arrel del servei DNS, l'entitat que els gestiona, el tipus de difusió que fan i el programari que utilitzen.

FIGURA 1.3. Llista de servidors arrel DNS i programari que utilitzen

Letter	IPv4 address	IPv6 address	Old name	Operator	Location	Software
A	198.41.0.4	2001:503:BA3E::2:30	ns.internic.net	VeriSign	distributed using anycast	BIND
B	192.228.79.201	2001:478:65::53	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S.	BIND
C	192.33.4.12		c.psi.net	Cogent Communications	distributed using anycast	BIND
D	128.8.10.90		terp.umd.edu	University of Maryland	College Park, Maryland, U.S.	BIND
E	192.203.230.10		ns.nasa.gov	NASA	Mountain View, California, U.S.	BIND
F	192.5.5.241	2001:500:2f::f	ns.isc.org	Internet Systems Consortium	distributed using anycast	BIND 9[3]
G	192.112.36.4		ns.nic.ddn.mil	Defense Information Systems Agency	distributed using anycast	BIND
H	128.63.2.53	2001:500:1::803f:235	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S.	NSD
I	192.36.148.17	2001:7fe::53 (testing)	nic.nordu.net	Autonomica	distributed using anycast	BIND
J	192.58.128.30	2001:503:C27::2:30		VeriSign	distributed using anycast	BIND
K	193.0.14.129	2001:7fd::1		RIPE NCC	distributed using anycast	NSD[4]
L	199.7.83.42 (since November 2007; originally was 198.32.64.12)[5]	2001:500:3::42		ICANN	distributed using anycast	NSD[6]
M	202.12.27.33	2001:dc3::35		WIDE Project	distributed using anycast	BIND

1.3.2 Instal·lació de l'aplicació servidor

Els usuaris de GNU/Linux poden buscar fàcilment per Internet paquets del client i del servidor DHCP usant eines com *apt-get* o *yum* i els repositoris de paquets apropiats segons quina sigui la distribució que utilitzin. A més, sempre es pot utilitzar algun cercador d'Internet per ajudar a localitzar tot allò que faci falta.

Un cop instal·lat el programari caldrà identificar què s'ha instal·lat. Quins paquets i què contenien. A vegades no s'instal·laran paquets sinó fitxers .tar, dels quals també caldrà saber-ne examinar el contingut. És important saber identificar quins dels components instal·lats corresponen a fitxers executables, quins a fitxers de configuració i quins a fitxers de documentació.

Tot servei instal·lat s'ha de configurar apropiadament i posar en marxa. Per tant, caldrà saber gestionar l'estat del servei (engegat, aturat...) i definir l'estat que ha de tenir en els diferents *runlevels* del sistema.

En definitiva, el procediment d'instal·lar usualment inclourà:

- Buscar el programari del servei (sigui en format de paquets .deb, .rpm o .tar) i descarregar-lo utilitzant l'eina apropiada segons quina sigui la distribució.
- Examinar el sistema per identificar quin programari i quins paquets relacionats amb el servei hi ha instal·lats.
- Identificar els components del servei: quins són els fitxers executables, de configuració i de documentació.

- Consultar i establir l'estat del servei (engegar i aturar) i saber establir l'estat per defecte per a cada *runlevel*.

1.3.3 Configuració per defecte del servei instal·lat

El servei DNS disposa usualment d'una configuració bàsica per defecte en instal·lar-se que acostuma a ser l'apropiada per a un servidor de noms només cau. A vegades simplement ve amb els fitxers de configuració buits, de manera que cal editar-los apropiadament abans de posar el servei en funcionament. En la configuració d'aquest servei s'usa el programari BIND (*Berkeley Internet Name Domain*) perquè és un dels més usats a nivell global. Cal identificar cadascun dels conceptes que descrits a continuació:

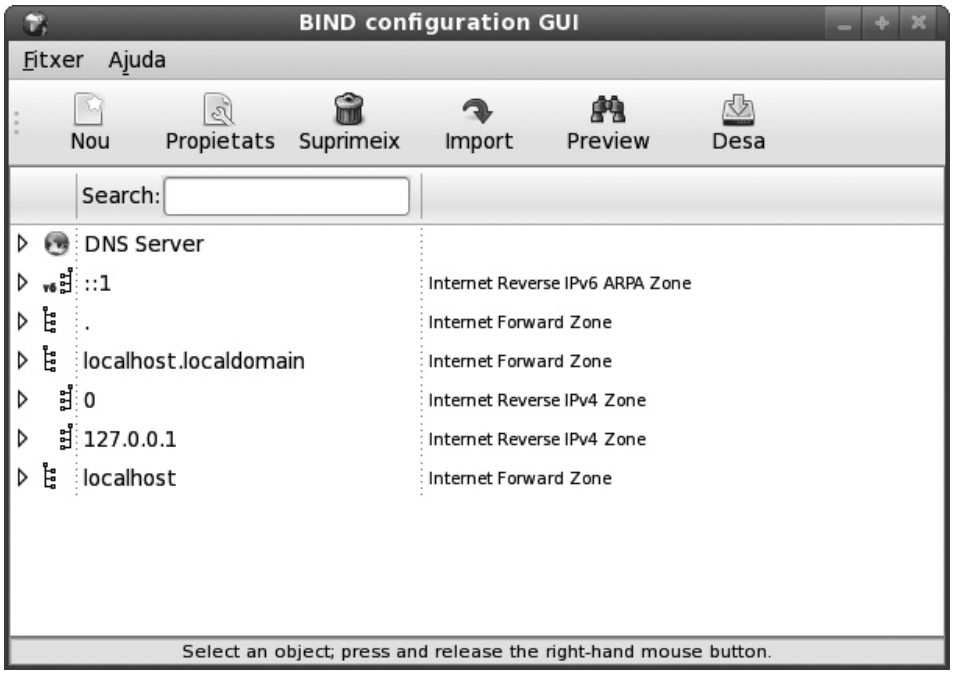
- Nom del servei: bind9 (localitzat a /etc/init.d/bind9).
- Fitxer de configuració: /etc/bind/named.conf.
- Directori dels fitxers de zona: /etc/bind.
- Llistat dels fitxers de zona predefinits que conté el directori anterior.
- Ubicació de fitxers d'exemple i pàgines de manual d'on poder obtenir una configuració inicial bàsica: /usr/share/doc/bind9 i /usr/share/man.

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

- **options**: s'hi defineixen les opcions genèriques del servidor DNS.
- **logging**: es defineix com serà el procés d'enregistrament dels *logs* del servei.
- **localhost_resolver**: permet definir el servidor DNS com un servidor només *cau*. És a dir, no és autoritari de cap domini, no gestiona cap domini, cap zona, no té fitxers de zona; l'única funció que fa és de servidor DNS *cau*.
- **internal**: permet definir les zones i zones delegades que es volen gestionar amb el servidor. Es donarà servei a les xarxes locals internes que es defineixen en aquesta secció.
- **external**: defineix el servei a oferir a clients externs al domini. És per oferir serveis DNS a clients exteriors.

La figura 1.4 mostra una eina gràfica que permet la configuració del servei de noms. En sistemes GNU/Linux és usual que els servidors es gestionin editant directament els fitxers de configuració. Es disposa, però, de miniaplicacins (*applets*) que permeten fer aquesta mateixa tasca des d'un entorn gràfic. Usualment no fan res de nou, és a dir, simplement serveixen per modificar els fitxers de text de configuració mitjançant un entorn gràfic més amable.

FIGURA 1.4. Miniaplicació gràfica de gestió del servidor BIND



Podem observar les zones que s'instal·len per defecte llistant el directori de treball per defecte del servei. Amb tota seguretat hi trobarem els fitxers corresponents a les zones arrel, localhost i loopback. A més, el paquet del servei segurament disposa de fitxers d'exemple de zona igual que disposava d'un exemple de fitxer de configuració del servei.

```
[root@host ~]# ls -l /etc/bind/
total 56
-rw-r--r-- 1 root root 2761 de juny  21  2019 bind.keys
-rw-r--r-- 1 root root  237 de juny  21  2019 db.0
-rw-r--r-- 1 root root  271 de juny  21  2019 db.127
-rw-r--r-- 1 root root  237 de juny  21  2019 db.255
-rw-r--r-- 1 root root  353 de juny  21  2019 db.empty
-rw-r--r-- 1 root root  270 de juny  21  2019 db.local
-rw-r--r-- 1 root bind  463 de juny  21  2019 named.conf
-rw-r--r-- 1 root bind  498 de juny  21  2019 named.conf.default-zones
-rw-r--r-- 1 root bind  156 de maig  27 20:09 named.conf.local
-rw-r--r-- 1 root bind  888 de maig  28 08:19 named.conf.options
-rw-r----- 1 bind bind   77 de maig  27 11:40 rndc.key
-rw-r--r-- 1 root root 1317 de juny  21  2019 zones.rfc1918
```

1.3.4 Exemple de configuració bàsica

La configuració bàsica i l'estructura de fitxers un cop s'ha instal·lat el servidor BIND permet familiaritzar-nos amb els seus components. L'estructura dels fitxers de configuració es basa en un fitxer principal, /etc/bind/named.conf, que està organitzat en 3 fitxers més:

```
root@server:~# cat /etc/bind/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";
root@server:~#
```

El contingut de cada un dels tres fitxers és el següent:

- /etc/bind/named.conf.options: conté les opcions del servei DNS.
- /etc/bind/named.conf.local: contindrà les zones noves que es volen afegir.
- /etc/bind/named.conf.default-zones: conté la zona arrel i les zones per defecte especificades al RFC 1912.

Directives

El llistat de totes les directives es pot consultar amb l'ordre:

man 5 vsftpdconf.

El contingut per defecte del **fitxer d'opcions** és el següent:

```
root@server:~# cat /etc/bind/named.conf.options
options {
  directory "/var/cache/bind";

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

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

  // forwarders {
  //  0.0.0.0;
  // };
  //========================================================================
  // If BIND logs error messages about the root key being expired,
  // you will need to update your keys.  See https://www.isc.org/bind-keys
  //========================================================================
  dnssec-validation auto;

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

Les opcions que apareixen en aquest fitxer són:

- Especificació el directori de treball del servei i els diferents fitxers de monitorització a utilitzar. Per exemple, fitxers per a volcats (*dump*), estadístiques (*statistics*) i estadístiques de memòria (*memstatistics*).
- Autenticació en les respostes DNS, si és el cas.
- Ports d'escolta del servei. En aquest cas també si es vol emetre respostes per a IPv6.

El contingut per defecte del **fitxer de configuració local** és el següent:

```
root@server:~# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

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

Aquest fitxer ve completament buit i és on s'han d'especificar les zones noves que es volen afegir al servidor DNS. Es recomana també afegir l'espai d'adreces privat (RFC 1918) si no s'especifiquen a les noves zones.

Espai d'adreces privat

L'espai d'adreces privat especificat al RFC1918 és el següent:

TAULA 1.1.

10.0.0.0	10.255.255.255	(10/8 prefix)
172.16.0.0	172.31.255.255	(172.16/12 prefix)
192.168.0.0	192.168.255.255	(192.168/16 prefix)

El contingut per defecte del **fitxer de configuració de zones per defecte** és el següent:

```
root@server:~# cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
  type hint;
  file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
  type master;
  file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
  type master;
  file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
  type master;
  file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
  type master;
  file "/etc/bind/db.255";
};
```

Aquest fitxer ve emplenat amb les zones per defecte. La més important és la primera, que és la **zona arrel** (fitxer /usr/share/dns/root.hints) i conté les 13 servidor arrels que hi ha a Internet. I les altres zones corresponen als espais d'adreces reservats especificats al RFC1912 i que el mateix document

recomana que apareixin (*certain zones should always be present in nameserver configurations*).

El contingut de la zona arrel és el següent:

```
root@server:~# cat /usr/share/dns/root.hints
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     March 13, 2019
;       related version of root zone:     2019031302
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
...
```

Espais d'adreces reservats

Els espais d'adreces reservats especificats al RFC1912 són els següents:

TAULA 1.2.

primary	localhost	localhost
primary	0.0.127.in-addr.arpa	127.0
primary	255.in-addr.arpa	255
primary	0.in-addr.arpa	0

1.4 Resolució, 'forwarding' i memòria cau

Tot sovint, en les aplicacions d'usuari i de sistema s'accedeix a recursos pel seu nom de domini. Per exemple, un client web requereix una determinada pàgina web, un navegador de fitxers vol accedir a unes carpetes d'una màquina remota que s'identifiquen pel nom de domini, el sistema ha de validar l'usuari en un servidor LDAP remot... En cada un d'aquests casos caldrà respondre una pregunta del tipus "A quina adreça IP correspon aquest domini?", "Quins són els servidors de noms del domini tal?", "Quins són els servidors de correus?". Aquestes preguntes no les responen les aplicacions individualment (el navegador web, el client d'autenticació...), sinó que utilitzen el *resolver* per fer-ho.

El *resolver* és la part client de l'arquitectura client/servidor del DNS. Ha d'atendre les necessitats de les aplicacions, confeccionar una consulta o *query*, enviar-la a un servidor DNS, obtenir la resposta i passar-la a l'aplicació pertinent. El *resolver* no és usualment una aplicació sinó un conjunt de biblioteques de funcions. Les aplicacions client es compilen i enllacen conjuntament amb aquestes biblioteques.

Els servidors que reben l'encàrrec de fer la resolució d'una consulta es poden comportar de maneres diferents en funció de com s'han configurat. Poden obtenir la resposta de la seva memòria cau, sol·licitar a un altre servidor de noms que sigui ell qui faci tota la feina de resolució (*forwarding*) o encarregar-se de fer la resolució pas a pas pel seu compte (*recursion*), consultant tans servidors de noms externs com faci falta.

En general podem catalogar el funcionament de la resolució en:

- memòria cau sí/no
- recursiu sí/no (recursiu/iteratiu)
- *forward* sí/no, combinat amb *forward only*

Fem una ullada al funcionament del mecanisme de resolució.

1.4.1 La resolució de noms

El mecanisme de resolució de noms DNS consta d'un client o *resolver* que realitzarà consultes (o *queries*) a uns servidors DNS.

Si el servidor disposa de la informació perquè forma part de la base de dades de la seva zona, emetrà una resposta **autoritativa**. Si disposa de la resposta perquè la té emmagatzemada temporalment (en un procés anomenat *cau*) també emetrà la resposta, però aquest cop de manera **no autoritativa**. Si no té informació del domini buscat, el servidor pot fer la consulta a altres servidors en un procés que pot ser **recursiu** o **iteratiu**. Sempre existeix un camí per trobar el domini buscat, que és preguntar als **nodes arrel** (*root servers*) de l'espai de noms de domini. Partint dels nodes arrel i recorrent l'arbre cap avall, es pot arribar al domini buscat, si és que existeix.

Sempre hi ha un camí a un domini existent partint del node arrel. Quan un servidor és consultat sobre un domini que desconeix (no és de la seva zona ni té la resposta en la memòria cau) pot escalar la pregunta a un servidor l'arrel (*root name server*). Això significa que els servidors arrel són crucials per al funcionament del DNS.

Exemple de resolució de noms DNS

Quina adreça IP té el *host* ns1.ioc.cat.? Si un estudiant australià intenta esbrinar això des del seu servidor de noms de Sydney, probablement acabarà preguntant per aquest domini a un dels nodes arrel. El node arrel desconeix el *host* ns1 del domini de l'IOC, però sí que

coneix tots els dominis de primer nivell (TLD). Per tant, l'arrel proporcionarà una llista amb els servidors de noms del domini cat. A continuació, el servidor de Sydney preguntarà a algun dels servidors de noms de la llista (del domini cat.) i obtindrà la llista de servidors DNS del domini ioc.cat. Preguntant als servidors d'aquest domini obtindrà l'adreça IP del *host* ns1 per al qual el domini ioc.cat. és autoritari (forma part de la seva zona).

Recursió i iteració

Quan el client o *resolver* emet una consulta al servidor DNS local (el servidor de noms que té configurat), aquest la pot tractar de manera **recursiva** o **iterativa**. De fet, el client *resolver* ja farà la consulta indicant si exigeix una resposta recursiva o iterativa. La diferència entre un mode i l'altre és com ha d'actuar el servidor DNS per obtenir la resposta quan no la té en la seva base de dades d'informació.

En el mode **iteratiu**, el servidor retorna la millor resposta possible basada en la seva informació local, sense preguntar a ningú més. En el mode **recursiu**, el servidor intenta trobar la resposta preguntant a tants altres servidors com calgui per obtenir-la.

Un servidor pot emetre les respostes següents:

1. Respon enviant la dada que li han sol·licitat (un nom de *host*, una adreça IP, la llista de servidors de noms, de servidors d'autenticació...).
2. Ha localitzat el domini buscat, però no disposa de la dada sol·licitada. Cal tenir en compte que es poden sol·licitar altres dades a part de l'adreça IP, per exemple, els servidors de correu que té el domini.
3. Finalment, pot ser que el domini sol·licitat no existeixi.

Recursió

Quan un servidor rep una consulta del client, mira la base de dades local de la seva zona. Si existeix la informació sol·licitada, la retorna. Si la dada no forma part de la seva zona, però la té emmagatzemada en la memòria cau (perquè ja ha realitzat amb anterioritat un consulta similar i ha emmagatzemat temporalment la resposta), també la retorna. Si la dada no forma part del seu espai de noms ni es troba en la memòria cau, el mode recursiu mana al servidor anar preguntant recursivament a altres servidors, apropant-se més a cada pas al domini sol·licitat. Si el servidor no coneix cap servidor més proper al domini buscat a qui preguntar, acaba preguntant als servidors de l'arrel.

Exemple de recursió

Si es consulta el domini www.inf.ioc.cat. i el servidor desconeix aquest domini, intentarà contactar amb un servidor de noms del domini inf.ioc.cat. Si tampoc sap com adreçar-se a aquest domini, intentarà contactar amb un servidor de noms de domini ioc.cat. Si també el desconeix, provarà de localitzar un servidor per al domini .cat. Si tampoc és el cas, es posarà en contacte amb un servidor de noms de l'arrel, . Un cop en l'arrel, sempre és possible accedir al domini buscat descendint per l'arbre de dominis.

Si tots els processos recursius acabessin preguntant als nodes arrel, aquests se saturarien. El servidor que ha rebut la consulta del *resolver* pregunta al node més proper al domini buscat. Si coneix algun servidor de noms més proper, li ho pregunta i evita d'anar a l'arrel.

Una altra manera d'evitar la sobrecàrrega dels nodes arrel és l'ús de la informació emmagatzemada de consultes anteriors, que es desa localment en la memòria cau del servidor.

Consulta d'informació delegada

Si es consulta l'adreça www.inf.ioc.cat. i el servidor que rep la consulta és el servidor de noms del domini ioc.cat., aquest no pregunta cap amunt (a cat. o a l'arrel .), sinó que obté de la seva pròpia base de dades la llista dels servidors de noms autoritaris de la zona delegada inf.ioc.cat., als quals preguntarà per obtenir una resposta.

Imagineu un alumne de Sydney, estudiant de l'IOC, que genera una consulta al servidor de noms del seu ISP australià per identificar el domini www.int.ioc.cat.. Probablement el servidor desconeix aquest domini i els propers, inf.ioc.cat. i ioc.cat. Però segurament en la memòria cau (per consultes prèvies) té la llista de servidors de noms autoritaris del domini cat. Serà a un d'aquests servidors (i no a un node arrel) a qui farà la consulta que li permetrà accedir de manera descendent al domini buscat.

Per tant, en el procés recursiu, el servidor de noms que rep la consulta del *resolver* ha de tornar una resposta que pot procedir de la seva base de dades de zona, de la memòria cau o de les respostes finals que ha obtingut preguntant recursivament a altres servidors propers al domini a consultar.

Fixeu-vos que un servidor que rep una consulta recursiva del *resolver* té la feina d'esbrinar per si mateix la resposta. Podria repetir la mateixa consulta al servidor més proper fent-la recursiva en lloc d'iterativa. Això exigiria a l'altre servidor fer tota la feina. Aquest plantejament, tot i que possible, es considera abusiu.

Usualment, el **client** consulta el seu DNS de manera **recursiva** i els **servidors** es consulten entre ells de manera **iterativa**.

Iteració

En el mode iteratiu, un servidor dóna la millor resposta possible basant-se en la pròpia informació (base de dades de zones locals i memòria cau). En cap cas no consulta cap altre servidor. Si no disposa de la resposta, lliura una llista amb els servidors més propers al domini que es busca. La llista pot ser d'un o més servidors i és tasca del servidor que ha fet la consulta decidir a quin d'ells tornar a preguntar (en el cas recursiu).

Els nodes arrel no accepten consultes recursives per evitar l'abús i la saturació.

Les consultes iteratives són usualment de servidor a servidor, però no del *resolver* al servidor. Si el *resolver* fes una consulta iterativa a un servidor, significaria que quan la resposta fos una referència a un altre servidor, el *resolver* hauria de fer una altra consulta. Generalment els *resolver* no tenen aquesta capacitat, simplement fan una consulta recursiva al servidor que tenen configurat i és aquest el que ha de fer tota la feina per obtenir la resposta.

El client *resolver* fa una consulta **recursiva** al seu servidor DNS local. Si el servidor DNS disposa de la resposta, la torna. Pot ser de la seva zona i serà una resposta **autoritativa** o pot tenir-la en la memòria cau i serà **no autoritativa**.
Si no disposa de la resposta, consulta **iterativament** altres servidors apropant-se al domini buscat. Cada servidor que consulta iterativament li pot proporcionar la resposta (autoritativa o no), si la coneix, o una llista de servidors DNS autoritatius per al domini indicat.
Finalment, s'obtindrà una resposta que pot ser aquella dada que es buscava o un error si el domini buscat no existeix.

Resolució inversa

Un *host* amb l'adreça IP 192.168.1.24 correspon al domini 24.1.168.192.IN-ADDR.ARPA.

El DNS proporciona un mecanisme per obtenir el nom de domini que correspon a una adreça IP determinada. Aquest mecanisme, anomenat **resolució inversa**, es basa en un domini especial anomenat IN-ADDR.ARPA. Hi ha protocols de xarxa que requereixen una resolució inversa correcta per funcionar bé i sovint s'utilitza com a mesura de seguretat per verificar l'existència de l'adreça IP en un domini.

La xarxa 172.16.32.0/24 correspon al domini ARPA següent: 32.16.172.IN-ADDR.ARPA.

S'ha ideat un domini anomenat IN-ADDR.ARPA que permet representar en forma de nom de domini totes les adreces IP possibles. El format són etiquetes numèriques del 0 al 255 que representen cada octet d'una adreça IP. Les etiquetes dels octets es concatenen en ordre invers i se'ls afegeix el sufix IN-ADDR.ARPA. Un nom de domini amb quatre etiquetes d'octets correspon a un *host*, un nom de domini amb menys etiquetes correspon a una xarxa.

En l'exemple següent es mostren els servidors de noms del domini ioc.cat i es fa una consulta de resolució inversa a cada un:

```
root@server:~# host -vt NS ioc.cat
Trying "ioc.cat"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65177
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;ioc.cat.     IN  NS

;; ANSWER SECTION:
ioc.cat.    900 IN  NS  dns2.nominalia.com.
ioc.cat.    900 IN  NS  dns1.nominalia.com.

;; ADDITIONAL SECTION:
dns2.nominalia.com. 4800  IN  A 81.88.63.48
dns1.nominalia.com. 254 IN  A 81.88.57.102

Received 108 bytes from 192.168.1.1#53 in 128 ms
root@server:~# host 81.88.57.102
102.57.88.81.in-addr.arpa domain name pointer dns1.nominalia.com.
root@server:~# host 81.88.63.48
48.63.88.81.in-addr.arpa domain name pointer dns2.nominalia.com.
root@server:~#
```

Exemple de configuració amb recursió

Vegeu les opcions que permeten configurar un servidor de noms en mode recursiu o en mode iteratiu. De fet, observant el fitxer de configuració podeu veure que és ben senzill:

```
# Fitxer /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        allow-query-cache { any; };
        allow-query { any; };
        recursion yes;

        dnssec-validation auto;

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

Podeu observar que es tracta simplement d'establir l'opció apropiada:

- ***recursion yes;*** estableix el mode de funcionamet com a recursiu.
- ***recursion no;*** estableix el mode de funcionament com a iteratiu.

Com es pot saber si el servidor funciona recursivament o iterativament? És ben senzill: un servidor iteratiu simplement pot resoldre consultes de la zeva zona o consultes prèvies que té emmagatzemades en la memòria cau. Però no pot resoldre consultes externes a la seva zona, ja que la recursió s'ha desactivat.

Per tant, podeu configurar el servidor iterativament (*recursion no;*) i comprovar que no es resolen consultes externes com gmail.com.. Tot seguit podem activar la recursió, *recursion yes;*, i fer la mateixa consulta externa. En aquesta ocasió s'ha d'obtenir el resultat buscat.

1.4.2 Ús de servidor 'forwarder'

Existeix un cas particular de funcionament dels servidors de noms que anomenem *forwarders*. Són servidors que podem anomenar informalment *l'encarregat*, o podem dir, encara més informalment, que "li passem el mort a tal" on *tal* és el ***forwarder***.

Imaginem, per exemple, una xarxa local corresponent al departament d'administració d'una empresa i que forma part d'una xarxa més gran, corresponent a l'empresa. En la xarxa d'administració s'ha instal·lat un servidor de noms només cau que no administra cap domini local. Es vol que aquest servidor tampoc generi consultes externes per motius que els administradors de xarxes creuen oportuns: per exemple, per temes de tallafocs, seguretat... Es vol que el servidor faci totes les consultes al servidor de noms de l'empresa, que serà qui farà la tasca de *forwarder*.

És a dir, quan es vol que un servidor de noms no realitzi consultes externes via recursió, sinó que totes les consultes les realitzi a un mateix servidor, és diu que es traspassen les consultes a aquest servidor encarregat. Aquest servidor és un *forwarder*.

> Es diu que un servidor fa ***forward*** quan passa totes les consultes externes a un altre servidor, que serà l'encarregat de resoldre-les.
> El servidor que rep l'encàrrec de fer aquesta feina de resolució s'anomena ***forwarder***.

Per configurar una estructura de resolució de noms amb un *forwarder*:

- En el servidor de noms que traspassarà les consultes a l'altre cal indicar quin servidor de noms serà el *forwarder*.
- En el que farà la funció de *forwarder* no cal indicar res. Simplement es trobarà que rep moltes consultes de resolució d'un *host* determinat, però no s'ha d'indicar res.

```
1 allow-query-cache { any;};
2 allow-query { any; };
3 recursion yes;
4 forward only;
5 forwarders { 192.168.122.1; 192.168.122.2};
```

En el fragment de codi anterior, extret del fitxer de configuració /etc/named.conf, podem observar les dues directives que indiquen al servidor que ha de traspassar totes les consultes a un servidor "encarregat". Anem a veure el significat de cada opció:

- ***forwarders***: indica l'adreça o adreces IP dels servidors als quals es farà *forward* de la consulta, és a dir, als quals s'encomanarà la tasca de resoldre-la. Com que l'especificació del protocol DNS recomana dos servidors de noms per domini, és usual trobar en aquesta opció almenys dues adreces IP. Aquestes corresponen als dos servidors d'un domini, els típicament anomenats *primari* i *secundari*.
- ***forward only***: si s'activa aquesta opció, el servidor funcionarà exclusivament en mode *forward*, de manera que qualsevol consulta serà tramesa al *forwarder*, idependentment de la memòria cau i de les zones pròpies.

1.4.3 Respostes de memòria cau

Es pot configurar un servidor de noms de domini perquè faci la funció de només cau. No gestiona cap zona, simplement atén les peticions dels *resolvers* client i les passa a altres servidors de noms. La seva funció és emmagatzemar en la memòria cau les respostes que obté abans de passar-les als clients. Això li permetrà que les

futures consultes que siguin repetides les pugui contestar directament en lloc de demanar-les a un altre servidor. Evidentment, aquest tipus de servidor no emet respostes amb autoritat.

La funció de memòria cau es pot activar i desactivar segons convingui. A més, es pot combinar amb les altres opcions de resolució per seleccionar el mode de funcionament del servidor. Les combinacions més usuals són:

- Si únicament es configura la funció de memòria cau es tractarà d'un servidor només cau.
- Si es combina la memòria cau i la recursió es farà resolució externa i es disposarà d'un cau local per poder contestar immediatament les consultes fetes amb anterioritat.
- El mateix passa si es combina la memòria cau amb el *forward*. El *forward* traspassarà la responsabilitat de resoldre les consultes externes a un altre servidor de noms. Disposar de la memòria cau activada permetrà respondre immediatament les consultes repetides.
- Desactivar la memòria cau significa que no s'emmagatzemen localment les respostes que es reben. Per tant, si es tornen a fer consultes que ja s'havien realitzat anteriorment caldrà tornar-les a resoldre pel mètode apropiat.

Si torneu a examinar el bloc d'opcions de configuració del mode de funcionament del servidor, extretes del fitxer /etc/bind/named.conf.options, observareu:

```
allow_query_cache { any;};
allow_query { any; };
recursion yes;
```

L'opció *allow-query-cache* permet indicar si s'activa o no la memòria cau i per a quines consultes. Les opcions que pot prendre són:

- *any;* indica que s'emmagatzemen en la memòria cau totes les respostes rebudes.
- *none;* no permet el funcionament de la memòria cau.
- *adreces-ip;* indica que les consultes que provinguin d'aquestes adreces-ip s'han d'emmagatzemar en la memòria cau. Les adreces-ip poden ser, de fet, combinacions dels tres conceptes següents: adreces IP, de xarxa o una llista-de-noms. Per exemple, 192.168.4.0/24;.

Autoritari, no autoritari i informació de memòria cau

Cada zona de l'espai dels noms de domini és gestionada per un o més servidors autoritaris per a la zona. Això significa que són els servidors que manen, que tenen l'última paraula respecte de la zona. De fet, significa que són els servidors que administren la zona. Aquests servidors es configurem com a **autoritaris** de

la zona. Les respostes que emeten a consultes referents a la seva zona porten un segell indicant que són autoritàries, que provenen de la base de dades distribuïda de l'espai de noms de domini.

Els servidors de noms guarden en una memòria cau les respostes que reben d'altres servidors. Aquesta informació també és utilitzada per elaborar respostes a consultes de dominis de fora de la zona de la qual són autoritaris. És a dir, quan un servidor rep d'un altre la llista de servidors autoritaris (en una consulta iterativa) per a una zona, aquesta llista s'emmagatzema a la memòria cau. Quan un servidor rep una resposta a una consulta també es guarda. Quan rep una resposta negativa, indicant que el domini de la consulta o el tipus de dada sol·licitat no existeix, també ho guarda. En aquest cas s'anomena *negative caching*.

Un servidor respon utilitzant la informació disponible en la base de dades de la seva zona (resposta autoritativa) o de la informació emmagatzemada en la seva memòria cau (provinent de consultes a zones externes efectuades anteriorment).

Quan rep una consulta a una zona externa que ja s'havia efectuat abans, s'utilitza la resposta de la memòria cau. També s'agafa de la memòria cau la llista de servidors autoritaris per a una zona més propera al domini que es busca, per tal de no preguntar als servidors arrel. Quan un servidor de noms respon utilitzant la informació de la memòria cau, la resposta és **no autoritativa**. No prové del servidor autoritari de la zona, sinó que s'utilitza una informació prèviament obtinguda (i que pot estar desfasada).

Per exemple, s'ha fet una consulta per al domini adm.ioc.cat i en el procés de resolució recursiu el servidor ha obtingut la llista de servidors autoritaris per als dominis cat. i ioc.cat. Si ara es demana al mateix servidor pel domini inf.ioc.cat. primerament provarà de resoldre aquest domini, però com que és desconegut, el següent domini més pròxim és ioc.cat. Aquest sí que el coneix, perquè el té emmagatzemat a la memòria cau de la resposta anterior. S'utilitzarà la llista de servidors autoritaris del domini ioc.cat. per obtenir una resposta o per continuar descendint per l'arbre de l'espai de noms.

Emmagatzemar informació de les respostes d'altres servidors en la memòria cau ofereix dos grans avantatges:

1. Incrementa la velocitat de resposta. Ja no cal anar a trobar la resposta a la font de dades de la zona, sinó que s'utilitza la informació d'una resposta anterior.
2. Evita la sobrecàrrega dels servidors arrel.

No cal anar al node arrel per cada consulta un cop que es disposa en la memòria cau d'informació més propera al domini a cercar. La utilització de la memòria cau té, però, un inconvenient que cal considerar: les dades no necessàriament són actualitzades. El DNS es fonamenta en una base de dades jeràrquica i distribuïda en la qual la informació es troba en els fitxers gestionats per cada servidor de zona. Una dada emmagatzemada en la memòria cau pot no reflectir la dada real, que ha estat modificada en el servidor autoritari de zona però que encara no s'ha propagat perquè es manté en la memòria cau fins que caduca el seu TTL (temps de vida).

Són servidors **autoritaris** els que administren una zona (tant el servidor primari o mestre com els secundaris o esclaus). Tenen accés a la informació **original** de la base de dades de zona.
Són respostes **no autoritàries** les que provenen de la informació desada en la memòria cau.

Fixeu-vos que si la informació de la memòria cau es desés indefinidament, els canvis que es fessin en els servidors autoritaris no es propagarien als altres servidors (perquè segurament ja disposarien d'una resposta en la seva memòria cau). Cal un mecanisme perquè la informació de la memòria cau caduqui transcorregut un cert interval de temps. Anomenem **TTL**, *Time To Live* o **temps de vida**, l'interval de temps que les dades han de perdurar en la memòria cau. Un cop transcorregut aquest temps, les dades s'eliminen. Si fa falta una dada, per obtenir-la caldrà fer una nova consulta.

Servidor només cau

La configuració completa d'un servidor DNS no és difícil, però és entretinguda. Cal crear cada fitxer de zona amb les entrades pertinents de cada *host* de la zona. Hi ha organitzacions petites que no necessiten configurar el servei DNS completament, en tindrien prou a tenir un servidor DNS local que permetés accelerar les consultes DNS que es fan a l'exterior.

Sabem que tota resolució de nom de domini comporta una consulta a un servidor DNS, usualment el del proveïdor de servei d'Internet (ISP). Es pot posar en marxa un servidor només cau en una xarxa local per proporcionar més eficiència a les consultes. El servidor només cau no administra cap zona, no té registres de recurs, simplement rep les consultes dels clients, les tramet al servidor DNS extern, rep les seves respostes, les desa en la memòria cau i les retorna al client.

El benefici d'aquest esquema és que el servidor només cau acumula en la memòria les respostes que va obtenint. En les consultes següents, si es demana pels mateixos dominis, ja no li cal passar la consulta a l'exterior, sinó simplement respondre des de la memòria cau. Evidentment, les seves respostes són sempre no autoritàries.

Un servidor **només cau** només emmagatzema les respostes d'altres servidors externs en la memòria, però no gestiona cap zona. No és autoritari, simplement augmenta l'eficiència quan rep consultes de les quals ja en sap la resposta (la té a la memòria cau).

Vegeu un exemple de configuració d'un servidor només cau:

```
root@server:~# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        allow-query-cache { any; };
        allow-query { any; };
```

```
        recursion yes;

        dnssec-validation auto;

        listen-on-v6 { any; };
};
root@server:~# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

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

En l'exemple anterior es pot observar que no es defineix cap fitxer de zona per ser administrada, excepte el fitxer de resolució directa dels servidors de noms de la zona arrel. Per tant, aquest servidor únicament atén peticions DNS com a intermediari i les desa a la memòria cau. El directori on emmagatzema temporalment la informació és /var/cache/bind.

1.5 Creació de zones

El propòsit principal d'un servei DNS és administrar una zona com per exemple una xarxa local amb tots els equips d'una organització, o un conjunt de zones d'una organització més complexa. Per fer això caldrà definir els fitxers de configuració del servei DNS i definir cada una de les zones de què es compongui la xarxa. També caldrà crear els fitxers corresponents a la resolució inversa de cada xarxa i del *loopback*.

Per crear una **zona pròpia** caldrà:

- Definir les zones en el fitxer de configuració del servei.
- Crear el fitxer de zona en què es defineix la resolució directa per a cada *host* de la zona i les característiques de la zona.
- Crear el fitxer de resolució inversa de la zona.

Les zones descriuen els equips que en formen part. És a dir, cada fitxer de zona és una base de dades que descriu els *hosts* que hi ha en la zona i la mateixa zona. Vegeu dos exemples de fitxers de zona abans d'explicar com descriure cadascun dels elements que hi pertanyen:

- Zona ioc.cat., corresponent a la resolució directa.
- Zona 2.0.10.in-addr.arpa., corresponent a la resolució inversa de la zona. Aquesta zona correspon a la xarxa 10.0.2.0/24.

```
;
; Fitxer de configuració del domini ioc.cat
;
$TTL 1D
ioc.cat.  IN SOA    server.ioc.cat. admin.ioc.cat. (1 3M 1M 1W 1D)
ioc.cat.  IN NS     server.ioc.cat.
server    IN A      10.0.2.10
www       IN A      10.0.2.11
ftp       IN CNAME  www
pc1       IN A      10.0.2.101
pc2       IN A      10.0.2.102
```

```
;
; Fitxer de configuració de la zona inversa ioc.cat
;
$TTL 1D
@    IN SOA server.ioc.cat. admin.ioc.cat. (1 3M 1M 1W 1D)
@    IN NS  server.ioc.cat.
10   IN PTR server.ioc.cat.
11   IN PTR www.ioc.cat.
11   IN PTR ftp.ioc.cat.
101  IN PTR pc1.ioc.cat.
102  IN PTR pc2.ioc.cat.
```

1.5.1 Tipus de registres

Aprofitar fitxers de zona

Els fitxers de zona de descripció del *loopback* i dels nodes arrel són pràcticament iguals per a totes les zones, de manera que usualment es copien d'una zona ja existent en lloc d'escriure'ls de nou.

El sistema de noms de domini és una base de dades jeràrquica i distribuïda en què cada servidor de noms gestiona la informació corresponent a la zona de la qual és autoritari. Cada zona conté informació dels *hosts* que la formen. La informació de zona s'emmagatzema en forma de **registre de recurs** o *resource record* (RR).

Aquest registre conté la informació que permet identificar cada nom de domini amb l'adreça IP corresponent, anomenat *forward mapping* o **resolució directa**. També conté la informació per identificar cada adreça IP amb el nom de domini corresponent, anomenat *reverse mapping* o **resolució inversa**. La informació de zones conté altres dades que permeten identificar els servidors DNS autoritaris per la zona, els servidors de correu...

La configuració d'una zona s'emmagatzema en un conjunt de fitxers anomenat *fitxers de zona*. L'especificació del DNS diu com han de ser aquests fitxers de zona i com s'hi han de descriure els registres de recurs (descripció de cada element que pertany a la zona).

> El conjunt dels registres de recurs de totes les zones de l'espai de noms formen la **base de dades** distribuïda jeràrquica del sistema DNS.

En qualsevol zona hi haurà almenys els **fitxers de zona** següents:

- Un fitxer amb les associacions dels noms de domini a adreces IP. Aquest fitxer defineix la resolució directa.

- Un fitxer per a cada subxarxa amb l'associació de cada adreça IP al seu nom de domini canònic. Defineix la resolució inversa.
- Un fitxer amb la definició de la resolució inversa del *loopback*.
- Un fitxer amb la descripció dels nodes arrel d'Internet.

Un cop que els fitxers de zona contenen tots els registres de recurs necessaris, cal configurar el servidor de noms perquè utilitzi aquests fitxers. Si bé la configuració dels fitxers de zona és estàndard (definida per l'especificació DNS), la configuració del servidor depèn del programa que s'utilitzi.

1.5.2 Registres de recurs

Cada fitxer de zona conté un conjunt d'entrades cadascuna de les quals defineix un **registre de recurs (RR)**. Els registres més usuals són SOA, NS, A, CNAME, PTR i MX. L'ordre en què apareixen és indiferent, però usualment és el mateix dels exemples. Cada línia té el format:

```
1 domini classe [ttl] tipus rdata:
```

- **domini** és el nom de domini que s'està definint.
- **classe** només pren actualment el valor "IN", per Internet.
- **ttl** és un camp opcional que descriu el temps de vida durant el qual cal emmagatzemar aquest registre en la memòria cau.
- **tipus** és el tipus d'RR que s'està definint.
- **rdata** és el valor que s'associa al nom de domini que es defineix.

Tot i que es pot definir un TTL en cada registre de recurs, el més usual és definir un TTL genèric per a totes les entrades del fitxer de zona. El servidor BIND 9 utilitza la directiva *$ttl* (per exemple: $ttl1 1h) per indicar el temps que els altres servidors de noms han de guardar en la seva memòria cau les respostes d'aquest servidor (una hora en l'exemple).

En la secció "Annexos" del web d'aquest mòdul trobareu altres tipus d'RR. També es poden trobar en l'especificació DNS.

Registre SOA

El registre de recurs **SOA** (*start of authority* o **inici de definició de zona amb autoritat**) diu que el fitxer de zona on es troba és la millor font de dades per a la zona, que el servidor de noms és autoritari per a la zona. Acostuma a ser el primer RR que hi ha en el fitxer de zona, tot i que no és obligatori. Per cada fitxer de zona hi ha d'haver només un registre SOA.

Punt final en el nom de domini

Posar o no el punt al final d'un nom de domini és important. Si acaba amb punt és un nom de domini absolut. Si no du punt és un nom relatiu i s'hi afegirà el domini per defecte al final.

Un registre SOA té el format:

```
nomDomini. IN SOA nsPrimari. admin.nsPrimari. (opcions–slaves)
```

Un exemple seria el següent:

```
inf.ioc.cat. IN SOA ns1.inf.ioc.cat. admin.ns1.inf.ioc.cat. ( 1 3h 1h 1w 1h )
```

La descripció de cada camp és la següent:

- **nomDomini.** indica el nom del domini que s'està definint i pel qual el servidor de noms és autoritari. Fixeu-vos en el punt final: és important posar-lo.
- **IN** indica que la classe és Internet.
- **SOA** informa que és un registre de recurs tipus SOA.
- **nsPrimari.** és el nom del *host* servidor de noms primari per a aquesta zona. Un altre cop pareu atenció al punt final.
- **admin.nsPrimari.** és l'adreça de correu electrònic de l'administrador del servidor de noms de domini, amb el format *usuari.servidor*. El primer punt que separa el nom d'usuari i el nom del servidor cal interpretar-lo com una arrova (*usuari@servidor*).
- **opcions-slaves** són paràmetres que s'indiquen entre parèntesis i que serveixen per definir com ha de ser la comunicació entre el servidor primari (o *master*) i els servidors secundaris (o *slaves*). A grans trets s'indiquen els conceptes següents:

  - *Serial*: el número de sèrie de la versió de les dades. A cada canvi de les dades de la zona, el número s'incrementa.
  - *Refresh*: temps a transcórrer entre cada refresc de dades del servidor secundari.
  - *Retry*: temps d'espera per tornar a intentar un refresc quan el servidor secundari ha fallat en l'intent d'actualitzar les seves dades des del servidor primari.
  - *Expire*: temps a partir del qual les dades del servidor secundari es consideren sense autoritat si no s'han refrescat abans.
  - *Minimum*: valor del TTL dels camps per defecte. Recordeu que a cada camp s'hi pot assignar un TTL específic. Segons la versió del servidor indicarà el TTL de les respostes negatives (*negative caching*), ja que el temps TTL es defineix per la directiva *$ttl*.

Formats de temps del BIND

BIND admet diferents formats per indicar el temps:

- #s: *seconds* (per defecte)
- #m: *minutes*
- #h: *hours*
- #d: *days*
- #w: *weeks*

Admet també combinacions, com per exemple: 3w12h, 2h20m...

Registre NS

El registre de recurs **NS** (*name server* o **servidor de nom**) defineix un servidor de noms autoritatiu per a la zona. Hi haurà tantes entrades NS com servidors de noms autoritatius hi hagi en la zona. L'estàndard DNS en recomana almenys dos (un de primari o *master* i un de seguretat, secundari o *slave*).

Un registre NS consta dels camps:

```
nomDomini. IN NS nameServer.
```

Un exemple seria aquest:

```
inf.ioc.cat. IN NS ns1.inf.ioc.cat.
```

La descripció de cada camp és la següent:

- **nomDomini.** indica el nom del domini que s'està definint.
- **IN** indica que la classe és Internet.
- **NS** descriu que es tracta d'un tipus de registre de recurs en què es defineix un servidor de noms.
- **nameServer.** és el nom del servidor de noms. Fixeu-vos un altre cop que tant *nomDomini.* com *nameServer.* acaben en punt per indicar que són noms de domini absolut o FQDN.

En la llista següent es pot veure part d'una resposta a una consulta *nslookup* per observar quins són els servidors de noms de Yahoo:

```
Authoritative answers can be found from:
yahoo.com       nameserver = ns2.yahoo.com.
...
ns8.yahoo.com   internet address = 202.165.104.22
```

Registre A

Un registre de recurs **A** (*address* o **adreça**) associa un nom de *host* a una adreça IP (resolució directa). Per cada nom de *host* de la xarxa caldrà disposar d'una entrada que associï el nom del *host* a la seva adreça IP.

Un registre A consta dels camps:

```
nomHost. IN A IP
```

Un exemple seria aquest:

```
mahatma.inf.ioc.cat. IN A 192.168.0.2
siddhartha           IN A 192.168.0.3
```

La descripció de cada camp és la següent:

- **nomHost.** indica el nom del *host* que s'està definint. Pot ser relatiu (sense punt final) o absolut (afegint el domini complert al final).
- **IN** indica que la classe és Internet.
- **A** informa que es tracta d'un tipus de registre de recurs de definició d'adreça IP.
- **IP** és l'adreça IP assignada al *host*.

Fixem-nos un altre cop que *nomHost.* acaba en punt per indicar que és un FQDN. Si no acabés en punt s'interpretaria com un nom relatiu al SOA que s'està definint actualment. Un *host* pot tenir més d'una IP assignada al mateix nom de *host*. Quan això passa s'anomena *multi-homed*. Simplement caldrà que hi hagi un registre A per a cada adreça IP. Constarà del mateix nom de *host* a l'esquerra de la definició i de la corresponent adreça IP a la dreta. Per exemple:

```
superserver.dom.com. IN A 10.0.0.1
superserver.dom.com. IN A 10.0.0.2
multihomed.ioc.cat.  IN A 172.12.0.1
                     IN A 172.12.0.2
```

Els noms definits en els registres de tipus A són noms **canònics**. Un *host* es pot identificar per més d'un nom, però només un és el nom canònic (original), la resta són **àlies**. Els noms canònics es defineixen amb el tipus de registre A. Els àlies es defineixen amb el tipus de registre CNAME.

A i CNAME

Compte! No s'han de confondre els registres de recurs A i CNAME: el registre A defineix *hosts*, mentre que el registre CNAME defineix àlies.

Registre CNAME

Els registres de recurs **CNAME** (*canonical name* o **nom canònic**) associen un àlies a un nom canònic.

Un registre CNAME consta dels camps:

```
nomHost. IN CNAME hostCanonicalName. | IP
```

Un exemple seria aquest:

```
ftp.inf.ioc.cat. IN CNAME mahatma.inf.ioc.cat.
tftp.inf.ioc.cat IN CNAME 192.168.0.2
```

La descripció de cada camp és la següent:

- **nomHost.** indica el nom de l'àlies que s'està definint.
- **IN** indica que la classe és Internet.
- **CNAME** informa que es tracta d'un registre de recurs de definició d'un àlies.

Exemple de host multi-homed

Es vol posar l'àlies *super1* i *super2* a cada una de les IP del host superserver.com (un *host* que té dues adreces IP assignades a aquest nom). Les entrades CNAME serien les següents:

- super1.dom.com. IN CNAME 10.0.0.1
- super2.dom.com. IN CNAME 10.0.0.2

- **hostCanonicalName | IP** és el nom de *host* canònic al qual s'assigna l'àlies. Fixeu-vos un altre cop que és un FQDN i que acaba en punt. Generalment, els registres CNAME tenen a la part dreta de la definició un nom canònic, però de vegades caldrà indicar-hi una adreça IP. Penseu en un *host multi-homed* amb múltiples adreces IP que a més té àlies. Si la definició fos pel nom canònic del *host*, no se sabria quina de les adreces IP correspon a l'àlies. En aquests casos, el CNAME apunta a una adreça IP.

La resolució dels àlies s'obté buscant l'entrada de l'àlies en el fitxer de zona. Amb l'entrada CNAME s'obté el nom canònic corresponent a l'àlies. Un altre cop es torna a buscar en el fitxer de zona, ara el nom canònic. Una entrada de tipus A proporcionarà l'adreça IP corresponent (àlies –> CNAME –> nom canònic –> A –> adreça IP).

Registre PTR

Un registre de recurs **PTR** (*pointer* o **punter**) associa una adreça IP al nom de *host* corresponent (resolució inversa). Cal una entrada PTR per a cada interfície de xarxa de la zona, per a cada adreça IP.

Un registre PTR consta dels camps:

```
1 ipInversa.in–addr.arpa. IN PTR hostName.
```

Un exemple seria aquest:

```
1 2.20.168.192.in–addr.arpa. IN PTR mahatma.inf.ioc.cat.
```

La descripció de cada camp és la següent:

- **ipInversa.in-addr.arpa.** indica l'adreça IP escrita en forma de domini in-addr.arpa per poder fer la resolució inversa. Les adreces IP s'escriuen al revés quan formen part del domini in-addr.arpa. Així, una IP 192.168.20.2 s'escriu 2.20.168.192.in-addr.arpa.
- **IN** indica que la classe és Internet.
- **PTR** informa que es tracta d'un registre de recurs de definició de la resolució inversa d'una adreça IP.
- **hostName.** és el nom de *host* FQDN assignat a l'adreça IP.

Registre MX

Un registre **MX** (*mail exchanger* o **servidor de correu electrònic**) defineix un servidor de correu. Es pot posar una entrada MX per a cada servidor de correu, però no és obligatori que n'hi hagi cap.

Un registre MX consta dels camps:

```
nomDomini. IN MX num mailServer.
```

Un exemple seria aquest:

```
inf.ioc.cat. IN MX 10 mailhost.inf.ioc.cat.
```

La descripció de cada camp és la següent:

- **nomDomini.** indica el nom del domini que s'està definint.
- **IN** indica que la classe és Internet.
- **MX** informa que es tracta d'un registre de recurs que defineix un servidor de correu per a aquest domini.
- **num** és un valor numèric que expressa el grau de preferència d'aquest servidor de correu respecte a altres servidors de correu del domini. El valor més baix és el que es prefereix. Són valors arbitraris que defineix l'administrador de xarxes.
- **mailServer.** correspon al nom FQDN del servidor de correu que s'està definint.

Observeu la llista de servidors de correu de Google a partir de:

```
root@server:~# host google.com
google.com has address 216.58.201.174
google.com has IPv6 address 2a00:1450:4003:80b::200e
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
root@server:~#
```

Exemples de registres de recurs (RR)

Les dues llistes següents mostren exemples dels fitxers de configuració per a la resolució directa i la resolució inversa de la zona ioc.cat. En el primer es defineixen dos servidors de nom, un encaminador, una impressora i dos *hosts*. El primer dels servidors de noms també fa les funcions de servidor de correu, web i FTP.

```
;Exemple de fitxer de zona ioc.cat
$TTL 3D
ioc.cat. IN SOA ns1.ioc.cat. admin.ioc.cat. { 23; 8H; 2H; 4W; 1D; };
      NS ns1.ioc.cat.
      NS ns2.ioc.cat.
      MX 10 correu.ioc.cat.
ns1.ioc.cat. A     192.168.0.5; servidor amb 2 ip
             A     172.16.20.5
ns2.ioc.cat. A     192.168.0.7; servidor dns slave
router       A     192.168.0.1; router. Nom relatiu
correu       CNAME ns1 ; alias correu
www          CNAME ns1 ; alias web
ftp          CNAME ns1 ; alias ftp
```

```
hp-7200c     A     192.168.0.2; impressora
pc01         A     192.168.0.50
pc02         A     192.168.0.51
```

En la llista següent es pot veure com es defineix una entrada PTR per a cada nom canònic definit en la resolució directa per a una subxarxa concreta. La subxarxa 192.168.0.0/24 utilitza el fitxer 0.168.192.in-addr.arpa per a la resolució inversa:

```
; Zona 0.168.192.in-addr.arpa.
; Exemple de fitxer de zona inversa ioc.cat
; correspon a la xarxa 192.168.0.0/24
$TTL 3D
ioc.cat. IN SOA ns1.ioc.cat. admin.ioc.cat. { 23; 8H; 2H; 4W; 1D;};
   NS ns1.ioc.cat.

5  PTR ns1.ioc.cat.
7  PTR ns2.ioc.cat.
1  PTR router.ioc.cat.
2  PTR hp-7200c.ioc.cat.
50 PTR pc01.ioc.cat.
51 PTR pc02.ioc.cat.
```

1.5.3 Configuració dels fitxers de zona

Exemple de configuració del servidor de noms

Per a una zona que es compon d'una única xarxa 192.168.20.0/24 amb el nom de domini inf.ioc.cat caldran els següents fitxers de zona:

- El fitxer de resolució directa inf.ioc.cat.zona.db.
- El fitxer de resolució inversa 192.168.20.zona.db o inf.ioc.cat.rev.zona.db.
- El fitxer de resolució inversa del *loopback*.
- El fitxer amb la informació dels nodes arrel del DNS, named.ca.

Els fitxers de zona contenen els registres de recurs que formen la base de dades de la zona. Cal configurar el servidor de noms per indicar-li quins són i on són aquests fitxers. Cada administrador anomena els fitxers com li plau o seguint l'estil marcat per l'aplicació servidor DNS que utilitza. Un exemple és anomenar els fitxers de zona amb el format *db.nomDomini* per al fitxer de resolució directa i *db.ipSubXarxa* per a la resolució inversa per a cada xarxa de la zona. En els exemples d'aquesta documentació s'utilitza la sintaxi *nomDomini.zona.db* per a la resolució directa, *nomDomini.rev.zona.db* per als de la resolució inversa i *ip.rev.zona.db* quan cal definir la resolució inversa d'altres xarxes.

Independentment de l'aplicació que s'utilitzi com a servidor de noms, caldrà configurar-la per dir-li on són aquests fitxers, com es diuen, si fan la funció de servidor autoritari per a la zona o no, si fan la funció de primari o secundari i altres opcions possibles.

Per cada fitxer de zona caldrà definir una entrada al fitxer de configuració global de BIND indicant el nom de la zona, el tipus i el nom del fitxer.

La sintaxi és:

```
zone nom_zona in { type master|slave|hint; file "nom_fitxer_zona"; };
```

Un exemple de configuració de zona podria ser:

```
zone inf.ioc.cat in { type master; file "inf.ioc.cat.zona.db;" }.
```

La descripció de cada camp és la següent:

- **zone nom_zona**: com es pot veure en l'exemple es defineix una zona corresponent al domini inf.ioc.cat.
- **type master | slave | hint**: el servidor serà primari (*master*) per a aquesta zona. Serà el que tindrà els fitxers amb les dades de la zona. El camp tipus pot prendre els valors *master*, *slave* i *hint*, que signifiquen el següent:
- **file nom_fitxer_zona**: indica el fitxer amb els registres de recurs de la zona. En l'exemple és el fitxer inf.ioc.cat.zona.db.

- *master*: el servidor té autoritat per a aquesta zona i gestiona els fitxers de zona.
- *slave*: el servidor és autoritari per a la zona, però obté les dades de la zona del servidor primari o *master*.
- *hint*: indica que es tracta de la informació corresponent als servidors de noms de la zona arrel. Aquesta informació té un tractament especial diferent del de les altres zones.

Cal parar especial atenció en la definició dels fitxers de zona per a la resolució inversa, utilitzant per exemple la xarxa 192.168.20.0/24. La zona s'anomena 20.168.192.in-addr.arpa, i el fitxer de zona, per exemple, db.192.168.20. El nom del fitxer conté l'adreça de xarxa en l'ordre natural, però el domini té els octets invertits perquè forma part del domini in-addr.arpa.

Vegeu l'exemple del fitxer de configuració del servei que inclou la definició de la zona directa ioc.cat. i la definició de la corresponent resolució inversa 2.0.10.in-addr.arpa. Aquestes definicions apunten als fitxers corresponents que descriuen els registres de recurs de cada una d'aquestes dues zones.

```
zone "ioc.cat" {
    type master;
    file "/etc/bind/ioc.cat.zona.db";
};
zone "2.0.10.in–addr.arpa" {
    type master;
    file "/etc/bind/ioc.cat.rev.zona.db";
};
```

1.5.4 Delegació de zona

El sistema de noms de domini DNS és una estructura jeràrquica i distribuïda. Hem vist com crear dominis i administrar-los en una zona que pot contenir altres subdominis que no s'hagin delegat. Per fer que l'estructura jeràrquica funcioni apropiadament cal poder delegar subdominis a altres entitats.

Delegar un subdomini implica transferir tota l'administració del domini delegat a una altra entitat. Un cop delegat, aquesta entitat és la responsable total de la seva

gestió. Caldrà establir el lligam entre el domini pare i el domini fill. Segurament caldrà realitzar els passos següents:

En el servidor de noms del domini fill:

- Generar els fitxers de zona directa i inversa i configurar apropiadament el servei.
- Verificar-ne el funcionament.

En el servidor de noms del domini pare:

- Realitzar la delegació.
- Verificar la delegació consultant registres del domini fill.

Optimitzar la consulta de la zona pare en el domini fill:

- Observar que des del servidor de noms fills no es disposa d'accés a la informació del domini pare. No hi ha lligam. Bé, sí, de fet, hi ha el mateix lligam que amb qualsevol altre domini. S'hi podrà accedir o no igual que a qualsevol altre domini.
- Fer del servidor de noms fill un servidor esclau de la zona pare.

Com a exemple pràctic creem una zona delegada inf.ioc.cat. corresponent a la xarxa 172.19.0.0/16. Aquests són els fitxers de zona:

```
; Fitxer de configuració dels hosts de la zona:
; inf.ioc.cat  (172.19.0.0/16)
$TTL 3D
@ IN SOA ns.inf.ioc.cat. admin.inf.ioc.cat. 1 3H 15M 1W 1D
          NS    ns
          MX    10 mailhost
ns        A     172.19.1.1
mailhost  A     172.19.1.2
printer   A     172.19.2.5
server    A     172.19.2.10
router    CNAME server
```

```
; zona 19.172.in–addr.arpa.
; inf.ioc.org  (reverse)  172.19.0.0/16
$TTL 3D
19.172.in–addr.arpa.  IN SOA ns.inf.ioc.cat. admin.inf.ioc.cat. 1 3M 1M 1W 1D
     NS  ns.inf.ioc.cat.
1.1  PTR ns.inf.ioc.cat.
1.2  PTR mailhost.inf.ioc.cat.
2.5  PTR printer.inf.ioc.cat.
2.10 PTR server.inf.ioc.cat.
```

El servidor de noms del domini inf.ioc.cat. es configura de manera anàloga a com s'han configurat els servidors en els exemples anteriors. Evidentment cal indicar quines són les zones que administra:

```
zone "inf.ioc.cat" {
  notify no;
  type master;
  file "inf.ioc.cat.zona.db";
};
zone "19.172.in–addr.arpa" {
  notify no;
  type master;
  file "inf.ioc.cat.rev.zona.db";
};
```

De fet, en el procés de delegació de zona no cal fer res d'especial en el servidor de la zona delegada. Només cal fer la configuració apropiada, posar-lo en funcionament i verificar-lo igual que es fa per a qualsevol altre servidor. On és, doncs, la màgia de la delegació? En el lligam que es fa del domini pare a la zona delegada.

Delegar una zona consisteix a indicar al fitxer de la zona pare quin és el servidor de la zona delegada.

- Això es fa amb un registre de recurs NS, indicant l'FQDN del servidor de noms de la zona delegada.
- Usualment caldrà a més un registre de recurs de tipus A, que indiqui quina és l'adreça IP del servidor de noms descrit en el punt anterior. Aquest és el registre de recurs que fa el **lligam** (*glue record*) que possibilita la "màgia" de la delegació.

Finalment, cal veure com es fa en la zona ioc.cat. per delegar. Cal afegir al fitxer de zona els dos registres de recurs que possibiliten la delegació:

```
; Fitxer de configuració dels hosts de la zona:
; ioc.org  (172.17.1.0/24)
$TTL 3D
@ IN SOA ns.ioc.cat. admin.ioc.cat. 1 3H 15M 1W 1D
          NS  ns
          MX  10 mailhost
ns        A   172.17.1.1
mailhost  A   172.17.1.2
server    A   172.17.1.10
...
; delegació de zona inf.ioc.cat.
inf.ioc.cat.    NS ns.inf.ioc.cat.
ns.inf.ioc.cat  A  172.19.1.1
```

Si analitzeu la primera de les línies de delegació, veureu que es defineix que el domini inf.ioc.cat. està gestionat per un servidor de noms anomenat ns.inf.ioc.cat. En la segona línia es fa el lligam físic que possibilita saber on és aquest servidor de noms del domini delegat. Aquesta segona línia indica que el servidor de noms és el corresponent a l'adreça IP 172.19.1.1.

Quan es pregunta al servidor de noms de la zona ioc.cat. pel *host* printer.inf.ioc.cat., el servidor busca en el seu fitxer de zona i detecta que les consultes que acaben en *inf.ioc.cat.* han de ser gestionades per un *host* anomenat ns.inf.ioc.cat. A continuació, intenta resoldre aquest nom consultant un altre cop el fitxer de zona i troba que el servidor de noms anomenat ns.inf.ioc.cat. correspon

a l'adreça IP 172.19.1.1. Quan ja sap on localitzar-lo continua la resolució (està fent una consulta recursiva) apropant-se al domini de destinació. Pregunta per *printer* al servidor ns.inf.ioc.cat. i d'aquest n'obté la resposta autoritativa.

Comprovació de delegació

Per comprovar la delegació de zona cal tenir present que primer cal verificar la zona delegada per si mateixa per tal que tot sigui correcte. Un cop és segur que funciona bé, cal verificar el lligam de la zona pare amb la zona fill. Això es pot realitzar fent consultes locals des del servidor pare de registres de la zona delegada.

Servidor delegat actuant com a esclau de la zona pare

Des del punt de vista de la zona delegada no hi ha cap lligam a la zona pare. És a dir, des del punt de vista d'un client de dins del domini inf.ioc.cat., demanar pel *host* smtp.gmail.com. o demanar pel *host* server.ioc.cat. implica el mateix procediment de resolució. Implica fer una consulta externa aplicant els mecanismes generals de resolució que s'han explicat en apartats anteriors. Sembla mentida, però el subdomini inf té tant (des)coneixement del seu domini pare com de qualsevol altre domini d'Internet.

Per tal d'implementar el traspàs de coneixement entre la zona pare i la zona delegada, cal fer del servidor de noms delegat un servidor **secundari** de la zona pare. Això és realment útil, ja que hi haurà sovint consultes des del subdomini inf referents a *hosts* del domini ioc.cat degut a que tots formen part d'una mateixa estructura organitzativa.

> Quan es tracta de subdominis dins d'una mateixa estructura organitzativa (una mateixa empresa o institució), és usual que els servidors de noms dels dominis delegats facin també de servidors **esclaus** del domini pare.
> D'aquesta manera poden respondre per si mateixos les consultes referents a tot el domini.

1.6 Transferències de zona

Els dominis d'Internet s'administren en zones, cada una gestionada per dos o més servidors de noms. Segons l'estàndard, cada zona té un servidor primari i almenys un servidor secundari. Ambdós són autoritaris per a la zona que administren. Caldrà, doncs, que aquests servidors disposin d'informació tan coherent com sigui possible, que comparteixin la mateixa informació. Això es fa mitjançant les transferències de zona.

Sovint, els servidors de noms actuen també com a memòria cau, emmagatzemant les respostes d'altres servidors per tal d'incrementar la seva eficiència. Quan emeten aquestes respostes actuen de forma no autoritària.

Sovint es confonen els conceptes relatius a la transferència de zones (servidor primaris i secundaris) amb els conceptes relacionats amb l'autoritat o no de les respostes. El següent destacat intenta aclarir cada un d'aquests termes.

Primari/secundari(s), també anomenats **master/slave(s)**: una zona és gestionada per un servidor primari (*master*) i un o més servidors secundaris (*slave*) o de seguretat.
Autoritari/no autoritari: els servidors d'una zona (el primari i els secundaris) són autoritat per a aquella zona que administren. Les respostes que emeten basant-se en la informació emmagatzemada en la memòria cau (informació procedent d'altres servidors de noms en lloc de procedir de la pròpia base de dades de zona) són no autoritàries.
Transferència de zona: la informació de la base de dades de la zona ha de ser coherent entre els servidors primari i secundaris. La transferència de zona és el mecanisme que s'estableix per fer que comparteixin la mateixa informació.

El servidor **primari** manté la base de dades de la zona i l'actualitza. Aquesta informació es copia als servidors **secundaris** utilitzant un procés de **transferència**.

Establir com i quan s'ha de fer aquesta transferència és important per proporcionar un bon servei DNS. Cal buscar un **compromís** entre **actualitzar** constantment la informació però consumir recursos excessius i no fer-ho però disposar d'informació **caducada**.

De fet, un servidor pot ser secundari per a una zona (o més d'una) i primari per a altres zones. Imaginem que el servidor ioc.cat. és primari per a la seva zona i ha delegat el domini alumnes.ioc.cat. a l'associació d'alumnes. El servidor de noms dels alumnes és primari per a la seva zona. Per agilitar les consultes al domini ioc.cat., l'IOC i els alumnes han acordat permetre que el servidor de noms de la zona alumnes.ioc.cat. faci també de secundari de la zona ioc.cat.

L'actualització de la informació entre el servidor primari i els secundaris és molt important. Establir correctament aquests **paràmetres** és un art. Un servidor amb informació antiga causa un mal funcionament a la xarxa, mentre que un servidor actualitzat constantment consumeix recursos excessius.

1.7 Extensions del protocol DNS

El protocol DNS és un protocol bastant antic, que s'ha anat adaptant als canvis que ha sofert Internet. Aquest apartat tracta els més importants, el servei amb adreces IP dinàmiques i la seguretat. El primer és degut a la manca d'adreces IPv4 i a la dificultat d'obtenir adreces IP públiques estàtiques (en la majoria dels casos són de pagament, almenys per a l'usuari final). El segon és la seguretat, on inicialment el protocol havia estat dissenyat sense tenir-la en compte.

1.7.1 Servei amb adreces IP dinàmiques

El servei de noms permet associar a una adreça IP un nom de domini. Així, per exemple, a l'adreça IP del servidor de l'usuari pere se li assigna el nom de host pere.ioc.cat en el domini de l'IOC. Ara bé, què passa si el *host* rep una IP dinàmica (de manera que la seva adreça IP pot variar)? Evidentment, en els fitxers de zona que lliguen les adreces IP amb els noms de domini cal saber prèviament l'adreça a usar i això no permetria assignar noms a adreces IP dinàmiques. Però també existeix un mecanisme anomenat DDNS o **DNS dinàmic** que permet fer actualitzacions dinàmiques en la base de dades de les zones.

> El procotocol o extensió **DDNS** (Dynamic DNS) permet realitzar **actualitzacions** en una base de dades DNS de manera dinàmica. De fet, es permeten afegir i eliminar registres de recurs dels fitxers de zona.
> Aquest protocol està descrit a l'RFC 2136 de l'IETF.

Utilitzant DDNS es poden afegir i eliminar registres a la base de dades d'una zona de manera que a mesura que assigna adreces dinàmiques als seus clients un servidor DHCP també pot anar realitzant peticions d'actualitzacions al servidor DNS per tal de que aquests clients disposin també de noms de domini.

1.7.2 Seguretat

Un dels principals problemes del protocol DNS és la seguretat, ja que és una cosa que no es va tenir en compte en el disseny inicial, on prevalia més que el disseny fos distribuït i escalable. Això va que aquest protocol es basi en la confiança que qui dona la informació és fiable i que aquesta informació és certa.

Si algú munta un servidor DNS en una xarxa privada juntament amb un servidor DHCP (que dona la configuració de xarxa als equips) al marge dels oficials que hi pugui haver en aquesta organització, i aquest servidor va ementent respostes falses, com per exemple donar unes altres IP per als bancs o el correu electrònic, és molt difícil detectar-ho. Aquest tipus d'atacs s'anomenen *Man In The Middle* (MITM). També es pot donar en el cas de xarxes WiFi obertes per a aquest propòsit (els coneguts *honey pots*) que exploten l'avarícia de la gent en obtenir alguna cosa de forma gratuïta. Aquest és un cas del caçador caçat.

Un altre cas encara més difícil de detectar és quan algun servidor DNS ha patit un atac i aquestes respostes es van actualitzant en altres servidors, fent que la informació que contenen en la seva memòria cau sigui fraudulenta. Aquest cas es coneix com **enverinament de la memòria cau DNS** (*DNS cache poisoning*, en anglès).

L'IETF va elaborar un conjunt d'especificacions conegut com a **Domain Name System Security Extensions** (DNSSEC) compatibles amb el protocol DNS.

Aquestes especificacions garanteixen l'autenticitat i la integritat de les dades DNS. No obstant, no garanteixen la confidencialitat, que, de fet, no és important ja que la informació que es transmet és de caràcter públic (les IP de cada domini).

El protocol o extensió **DNSSEC** permet garantir l'**autenticita**t i la **integritat** en les consultes a servidors DNS. Aquestes extensions estan descrites en el RFC 4033, 4034 i 4035.

Aquest sistema utilitza signatures digitals basades en criptografia de clau pública. Cada zona DNS té el seu parell de clau pública-privada amb la qual es van signant les dades de les consultes i respostes DNS a través d'un mecanisme de confiança que arriba fins als servidors arrels (cadena de confiança). La zona arrel del protocol DNS està signada des del 2010, així com la majoria de gTLD i ccTLD.

2. Instal·lació i administració de serveis de configuració automàtica de xarxa

El servei **DHCP** permet la configuració d'adreces IP, màscares, passarel·les per defecte (*gateways*) i moltes altres opcions de configuració de manera totalment dinàmica.

DHCP

DHCP és l'acrònim de Dynamic Host Configuration Protocol, en català, protocol de configuració dinàmica d'equips.

Una manera planera d'entendre el DHCP és imaginar que, en arrencar, els equips clients fan un crit per la xarxa i pregunten "Que hi ha algú?", "Qui soc jo?". El servidor del DHCP els contesta proporcionant-los tota la informació necessària perquè sàpiguen qui són i com han de configurar els seus paràmetres de xarxa.

L'administrador de xarxa té la tasca de configurar els equips que la componen. Això significa configurar els servidors, els equips clients, concentradors, encaminadors... Cada equip de la xarxa s'ha d'identificar amb l'adreça IP corresponent i la màscara de xarxa, i generalment disposarà d'un camí d'accés a Internet.

Tant els usuaris com els serveis requeriran l'accés a altres equips identificant-los pel nom de domini en lloc de fer-ho per l'adreça IP, que és més difícil de recordar. Fer això equip per equip resulta una feina feixuga i repetitiva si no es disposa de serveis de xarxa que la facilitin.

2.1 Configuració automatitzada de xarxa

El servei DHCP proporciona un mecanisme de configuració centralitzat dels equips de la xarxa. En lloc de configurar un per un els equips de xarxa amb adreces i valors estàtics, un servidor DHCP anirà assignant als equips clients els valors que els corresponguin. Aquesta assignació es fa per un període de temps finit, passat el qual caldrà renovar-la.

Els principals avantatges d'utilitzar DHCP són, d'una banda, evitar conflictes d'adreces IP (adreces repetides i adreces errònies), ja que passar equip per equip a canviar la configuració és molt més pesat i propens a l'error que fer-ho editant un sol fitxer de configuració en el servidor DHCP; i, de l'altra, que fer l'administració centralitzada representa un estalvi de temps i de feina.

Avantatges del DHCP

El servei DHCP té diversos avantatges:

- Evita errors i conflictes IP.
- Centralitza l'administració.
- Estalvia temps.
- Simplifica l'administració.

El servei DHCP simplifica l'administració de la configuració dels equips de xarxa fent-la centralitzada, dinàmica i amb concessions per períodes de temps finits.

La concessió dinàmica d'adreces IP i d'altres paràmetres de configuració de xarxa es realitza per un període de temps determinat, que varia en funció de les necessitats del client i del servidor.

Exemples d'ús del servei DHCP

Els següents són alguns exemples d'ús del servei DHCP:

- En una biblioteca que admet connexions Wi-Fi, els clients obtindran concessions per un temps reduït, per exemple, minuts.
- Un usuari d'Internet que rep al seu equip de casa una adreça IP dinàmica del seu proveïdor d'accés a Internet (ISP) tindrà una concessió que segurament serà per hores.
- En la xarxa corporativa d'una empresa que s'ha configurat dinàmicament usant DHCP, els equips rebran concessions dinàmiques per períodes de temps llargs, per exemple, de dies.

2.1.1 Configuració d'un equip de xarxa

Qualsevol equip que pertany a una xarxa requereix que es configuri amb uns paràmetres mínims, que són l'adreça IP, la màscara i la porta d'enllaç per defecte (també anomenada *gateway*). L'adreça IP identifica l'equip de manera única i la màscara permet determinar la xarxa o subxarxa en què es troba l'equip. Amb aquests dos paràmetres n'hi ha prou per tenir connectivitat en la xarxa. Si es vol disposar d'accés fora de la xarxa pròpia (per exemple, a Internet o a la resta de la xarxa corporativa) cal definir també l'encaminador o *gateway*. A part de la configuració bàsica, els equips poden necessitar (de fet, ho necessiten) més paràmetres de configuració, com, per exemple, el nom del *host*, els servidors DNS a usar, el fitxer d'iniciació per a arrencades PXE...

Tot equip de xarxa necessita disposar d'una **adreça IP** que l'identifiqui de manera única a la xarxa. Li cal també una **màscara** per poder distingir en l'adreça IP la part d'**adreça de xarxa** i la d'**adreça de *host***. Finalment, és imprescindible disposar de l'adreça de la **porta d'enllaç predeterminada** o passarel·la per defecte (*gateway*), per disposar d'accés a xarxes externes.

Exemple de configuració de xarxa d'un equip domèstic

La majoria d'usuaris disposen a casa d'un equip (o més) connectat a un encaminador (*router*) que proporciona l'accés a Internet. Aquest equip està configurat com a client DHCP i en iniciar-se rep la configuració de xarxa de l'encaminador. Podeu comprovar a casa quina configuració teniu. Una configuració d'exemple podria ser:

```
1        Adreça IP. . . . . . . . . . . . .: 192.168.1.33
2        Màscara de subxarxa . . . . . . . : 255.255.255.0
3        Porta d'enllaç predeterminada . . : 192.168.1.1
4        Servidor DHCP . . . . . . . . . . : 192.168.1.1
5        Servidors DNS . . . . . . . . . . : 80.58.61.250
6                                            80.58.61.254
```

L'inconvenient de la configuració estàtica

La configuració estàtica implica configurar els equips un a un. Fins i tot encara que es tingui accés remot als equips (per Telnet o SSH), com que cal modificar la configuració de xarxa, no es pot fer assegut des de l'equip de l'administrador, sinó que cal anar equip per equip a modificar la configuració.

Aquest procés de configuració cal que es faci per a cada equip de la xarxa. Fer-ho manualment implica configurar equip per equip sense cometre errades en teclejar les adreces i les màscares. Qualsevol canvi en l'estructura de la xarxa, com per exemple redefinir les subxarxes o modificar algunes adreces IP, significa tornar a configurar manualment els equips implicats. És evident que tota aquesta feinada

no és agradable per a l'administrador de xarxa (és molt avorrida!). Tant si la xarxa corporativa consta de pocs equips com de molts, cal una solució que permeti automatitzar la configuració de xarxa de cada equip de manera centralitzada.

Les opcions de configuració de xarxa es poden assignar a cada equip **estàticament** o es poden configurar de manera **dinàmica** utilitzant DHCP.

Com a administradors de xarxa, la gestió centralitzada que proporciona DHCP ens permet modificar la xarxa afegint, eliminant i redefinint equips amb un cost mínim.

2.1.2 Tipus d'assignacions d'adreces IP

Cada equip de xarxa té assignada una adreça IP que l'identifica de manera única dins de la xarxa. La composició de l'adreça IP i la màscara determinen la xarxa o subxarxa a la qual pertany. A més, es configuren altres paràmetres de xarxa com la porta d'enllaç predeterminada, servidors DNS... Això es pot configurar manualment anant equip per equip i introduint aquesta informació.

Quan l'adreça IP i els altres paràmetres necessaris de configuració de la xarxa es configuren equip per equip, manualment, es diu que tenen una adreça **IP estàtica**.

Reconfiguració d'una xarxa

Imagineu de quin humor estarà l'administrador d'una xarxa corporativa de 1.000 equips amb adreces estàtiques quan cal reconfigurar-la en un cap de setmana!

Quan la configuració de xarxa d'un equip no es fa manualment i localment en l'equip sinó que es fa per mitjà d'un servidor DHCP, es diu que l'equip utilitza una adreça **IP dinàmica**. Per realitzar configuracions de xarxa dinàmicament caldran un o més servidors DHCP (a manera de redundància), que proporcionaran la configuració als equips clients (els que cal configurar). Per tant, serà una estructura client/servidor. Les adreces IP dinàmiques que rep el client les podem classificar en dues categories: **assignació dinàmica de rang** i **assignació fixa**.

El servidor DHCP disposa d'un rang d'adreces que pot assignar als clients que demanen una adreça IP. Quan el servidor assigna una adreça qualsevol del rang al client (a l'atzar) es tracta d'una assignació dinàmica de rang. El client no sap quina adreça IP tindrà i no hi ha manera de predir quina se li concedirà en una futura configuració. A cada nova assignació, l'adreça IP pot ser diferent.

MAC

Cada interfície de xarxa s'identifica de manera única físicament per l'adreça MAC (*media acces control* o adreça d'accés al medi).

Una assignació fixa es produeix quan el servidor DHCP assigna sempre la mateixa adreça al client. Per assignar sempre la mateixa adreça IP al client cal que el servidor pugui identificar inequívocament el client (per l'adreça MAC). El servidor disposa d'una taula amb les correspondències entre les adreces MAC i les adreces IP fixes.

Quan la configuració de xarxa d'un equip es fa per mitjà d'un servidor DHCP es diu que utilitza una adreça IP **dinàmica**. Aquesta adreça pot variar dins d'un **rang** d'adreces disponibles del servidor DHCP o pot ser **fixa**.

DNS dinàmic

Hi ha serveis de DNS dinàmic (DDNS) que permeten assignar un nom de domini a equips amb adreça IP dinàmica.

Els avantatges de disposar d'una adreça IP fixa són que la vostra identificació a Internet (la vostra adreça IP) no varia i tothom us pot identificar sempre per la mateixa IP. Podeu proporcionar serveis a altres equips i els clients us identifiquen sempre amb la mateixa adreça sense haver de recordar en cada moment quina adreça IP teniu avui (com passa en el cas d'una IP dinàmica).

2.2 Funcionament del protocol DHCP

El protocol DHCP està descrit, com la majoria de protocols de xarxa, per un document oficial anomenat RFC. Aquest document ha sofert una evolució al llarg dels anys per anar-se adaptant a les necessitats de cada moment. Tot protocol implica un diàleg entre els equips que intervenen en un procés. Ens caldrà, doncs, analitzar quin és i com es produeix aquest diàleg. Finalment es descriurà el significat de termes tan usuals en el DHCP com *rangs*, *exclusions*, *concessions* i *reserves*.

RFC

Request for Comments (RFC) són memoràndums sobre noves investigacions, innovacions i metodologies relacionades amb les tecnologies d'Internet. Els publica l'Internet Engineering Task Force (IETF) i defineixen a escala mundial els protocols i les seves revisions. És a dir, són les publicacions oficials que descriuen els protocols.

2.2.1 Evolució del protocol DHCP

L'RFC 951 és el document base que descriu el protocol BOOTP.

El servei DHCP és un servei del tipus client/servidor que proporciona la configuració de xarxa als clients que ho sol·liciten. Proporciona els paràmetres bàsics de xarxa com l'adreça IP, la màscara de xarxa, la porta d'enllaç i altres paràmetres necessaris per a la connexió a una xarxa IP. Es tracta d'un protocol de la capa d'aplicació del model TCP/IP.

El protocol DHCP està basat en l'arquitectura de serveis client/servidor i utilitza com a transport el protocol UDP de la pila de protocols TCP/ IP. El servidor DHCP es comunica amb els clients utilitzant paquets UDP, que rep en el seu port 67 i envia al port 68 del client.

La configuració dinàmica d'equips de xarxa es va iniciar amb el protocol BOOTP (BOOT Strap Protocol o protocol d'arrencada). Era un protocol més bàsic que principalment permetia definir l'adreça IP, la màscara de xarxa i la passarel·la per defecte per al client. El BOOTP (RFC 951, any 1985) és un protocol pensat per

proporcionar automàticament la IP a clients de xarxa en el procés d'arrencada. Originàriament s'utilitzava per a estacions de treball sense disc que obtenien la configuració de xarxa del protocol BOOTP i també obtenien el nom d'un fitxer d'arrencada que s'havia de baixar per mitjà del TFTP, que usualment era el sistema operatiu.

El BOOTP va donar pas al protocol DHCP, que n'és una evolució amb moltes més prestacions. El DHCP sorgeix l'octubre de 1993 mitjançant l'RFC 1531. Ràpidament evoluciona gràcies a diversos RFC, com l'RFC 1541 (el mateix 1993), que serà substituït per l'RFC 2131, el març del 1997. Aquest document és la base del protocol DHCP actual. A grans trets, el protocol es descriu en l'RFC 2131 per a xarxes Ipv4, el conjunt d'opcions de configuració de DHCP es descriuen en l'RFC 2132 i l'especificació del DHCP per a xarxes Ipv6 és en l'RFC 8415.

RFC del DHCP

Principals RFC dedicats al DHCP:

- RFC 2131, març 1997: "DHCP: Dynamic Host Configuration Protocol"
- RFC 2132: "DHCP options"
- RFC 3396: "Encoding long options"
- RFC 4361: "Node-specific client identifiers for DHCPv4"
- RFC 8415: "DHCPv6: Dynamic Host Configuration Protocol Ipv6"

2.2.2 El model funcional del protocol DHCP

El protocol DHCP descriu el diàleg que es produeix entre client i servidor per a la concessió de configuracions IP. En una xarxa amb configuració d'equips dinàmica, un o més servidors DHCP escoltaran les peticions dels clients en el port 67. Els clients DHCP sol·licitaran al servidor DHCP una configuració IP i començarà un procés de negociació que ha d'acabar (si tot va bé) amb la concessió d'una adreça IP al client. Els servidors parlen al port 68 dels clients.

La negociació que s'estableix es pot definir a grans trets de la manera següent:

1. El client sol·licita una adreça IP (de fet, una configuració de xarxa).
2. El servidor mira les adreces IP disponibles dins del rang d'adreces dinàmiques de què disposa per concedir i n'ofereix una al client.
3. Si el client l'accepta, envia una sol·licitud al servidor per fer-la seva.
4. Si al servidor li sembla bé, accepta la petició del client i li confirma que pot utilitzar aquesta adreça IP, que l'hi concedeix per un període de temps limitat.

Ports DHCP

El protocol DHCP utilitza UDP en la capa de transport. Utilitza dos ports:

- Port 67, on escolta el servidor.
- Port 68, on escolta el client.

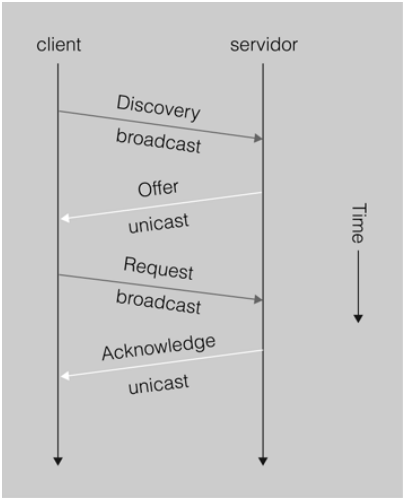
La concessió de l'adreça IP és per un període de temps establert pel servidor. Això significa que, transcorregut aquest període, el client haurà de renegociar la concessió en un procés similar al descrit anteriorment. En la figura 2.1 ("Model funcional del protocol DHCP") es pot veure el diàleg de quatre fases entre el client i el servidor.

UDP en les transmissions DHCP

L'intercanvi d'informació entre client i servidor no és gaire gran (poc volum de dades) i no requereix un flux permanent (una conversa continuada). És per això que el protocol que s'utilitza en les transmissions DHCP és l'UDP.

El procés real, però, és més detallat. El podem repassar. Consta principalment de quatre parts: la petició del client o *discovery*, l'oferta del servidor o *offer*, l'acceptació de l'adreça IP pel client o *request* i la confirmació del servidor o *acknowledgement*. A part d'aquest tipus de missatges, el protocol DHCP en defineix d'altres com el de petició d'informació o *information* i el d'alliberament de l'adreça IP o *releasing*.

FIGURA 2.1. Model funcional del protocol DHCP



Els següents són els tipus de paquets DHCP:

- *DHCP discover*
- *DHCP offer*
- *DHCP request*
- *DHCP ack* / *DHCP nack*
- *DHCP decline*
- *DHCP release*
- *DHCP information*

DHCP 'discover'

En un procés de configuració dinàmica d'un client de DHCP, el paquet *DHCP discover* és el primer que s'envia. L'envia el client per tal de demanar una configuració IP a algun servidor. Generalment, el client s'acaba d'inicialitzar i vol obtenir una configuració dinàmica de xarxa. El client no sap a quina xarxa pertany (no té adreça IP ni màscara de xarxa) ni tampoc sap quins servidors DHCP hi ha en la xarxa (si n'hi ha cap).

Una difusió o *broadcast* s'adreça a la IP 255.255.255.255 o a l'adreça MAC FF:FF:FF:FF:FF:FF, que és acceptada per tots els equips.

Per tant, el client genera un paquet de difusió (*broadcast*) destinat a tots els equips de la xarxa on sol·licita una configuració IP. En la xarxa pot haver-hi cap, un o més d'un servidor DHCP per atendre aquesta petició. És responsabilitat de l'administrador de xarxes configurar correctament l'estructura i els serveis de xarxa, de manera que si defineix clients de DHCP hi hagi servidors DHCP que atenguin les seves peticions.

DHCP 'offer'

En rebre una sol·licitud de configuració d'un client (*DHCP discover*), un servidor DHCP mira d'atendre-la proporcionant una adreça IP del rang d'adreces dinàmiques que gestiona (hi pot haver més d'un servidor DHCP en la mateixa xarxa).

El servidor tracta d'assignar una IP del conjunt o rang (també anomenat *pool*) d'adreces dinàmiques que gestiona. Per fer-ho, ha de mirar quines de les adreces li queden lliures i disponibles per concedir al client. Cada vegada que el servidor concedeix una adreça IP a un client ho anota en un fitxer de registre de les concessions efectuades. Cada vegada que finalitza una concessió el servidor pot tornar a utilitzar l'adreça IP per a un altre client.

Diversos servidors DHCP

Es pot configurar més d'un servidor DHCP, tant per a còpia de seguretat o *backup* com per incrementar el rendiment en compartir la càrrega de les peticions.

Tota **concessió** (o *lease*) DHCP és per un període determinat de temps, i un cop transcorregut cal renovar-la.

El mecanisme que utilitza el servidor per escollir l'adreça IP dins del conjunt d'adreces IP disponibles varia en funció del programa de servidor que s'utilitzi. A més, es poden configurar innumerables opcions del servidor per establir com s'han de fer les concessions. Un cas típic és el de les adreces fixes. A un determinat client se li assigna sempre la mateixa adreça IP. Per això cal disposar de la llista d'adreces MAC dels clients als quals es vol assignar una adreça IP fixa.

El servidor selecciona una adreça IP disponible i la reserva per al client (encara no està assignada). Tot seguit envia un paquet *DHCP offer* (unidestinació o *unicast*) al client amb tota la informació de configuració requerida. L'adreça IP i MAC origen identifiquen el servidor que fa l'oferta. El destinatari s'indica per la seva adreça MAC (que és coneguda). El camp IP del destinatari és l'adreça IP que el servidor ofereix (penseu que el client encara no té adreça IP). Un altre concepte important és per quant temps es realitza la concessió. El paquet inclou camps per completar la resta de configuració de xarxa, per exemple, la porta d'enllaç per defecte, els servidors DNS...

Tipus d'adreçament

Hi ha diversos tipus d'adreçament:

- Unidestinació o *unicast*: a un equip
- Multidestinació o *multicast*: a un conjunt d'equips
- De difusió o *broadcast*: a tothom

DHCP 'request'

Quan el client rep una oferta de configuració IP per part d'un servidor, la pot acceptar o rebutjar. Si el client no accepta l'oferta, simplement realitzarà un nou *DHCP discovery*. Això és suficient perquè el servidor s'adoni que l'oferta ha estat rebutjada.

Si el client accepta l'oferta, ho ha de comunicar al servidor. El mecanisme per fer-ho és mitjançant un paquet *DHCP request* enviat un altre cop per difusió. A hores d'ara, el client encara no disposa de l'adreça IP per utilitzar-la. El servidor l'ha reservat, però encara no ha donat el sí definitiu perquè sigui concedida al client.

El motiu pel qual el client demana quedar-se la concessió (*DHCP request*) que ha rebut utilitzant difusió és fer públic a tothom de la xarxa que ha acceptat una oferta d'un servidor DHCP concret. Recordeu que la petició del client es fa per difusió i, per tant, pot rebre ofertes de diferents servidors DHCP. Quan accepta

una de les ofertes, no ha de dir res als altres servidors que ha refusat. Simplement fent pública quina oferta accepta, la resta de servidors DHCP entenen que la seva oferta s'ha rebutjat.

DHCP 'acknowledgement' (DHCPACK/DHCPNACK)

L'últim pas en una negociació DHCP bàsica el realitza el servidor quan finalment autoritza la concessió enviant el paquet DHCPACK (*DHCP akcnowledgement*). A partir d'aquest moment, el client ja pot fer ús de l'adreça IP i de la configuració de xarxa rebuda. DHCPACK inclou tota la informació referent a la durada de la concessió i les dades necessàries per gestionar quan expira.

ACK i NACK

ACK i NACK són dos acrònims usuals en el món de la informàtica. Signifiquen conformitat (acceptació) i no conformitat (refús) respectivament.

El servidor anotarà en el registre de concessions la que acaba de realitzar i en detallarà tots els aspectes, en especial el temps de concessió. El paquet d'acceptació de la concessió DHCPACK és un paquet unidestinació adreçat a la MAC del client. Recordeu que el client encara no disposa d'una adreça IP vàlida; en disposarà en rebre el DHCPACK.

Exemple de mala configuració d'un equip

Un exemple de mala configuració és la d'un equip que s'ha engegat amb una adreça IP estàtica errònia que se solapa amb les adreces IP que reparteix el servidor. El mecanisme usat per comprovar si l'adreça IP ja està essent utilitzada és un *ping*. Si no respon ningú és que està lliure (segurament).

Quan un servidor DHCP detecta que la IP que havia reservat per a un client i que li anava a concedir ja està en ús (per una configuració incorrecta), el servidor envia al client un paquet DHCPNACK i indica la no autorització de la concessió. El client que rep un DHCPNACK ha de tornar a iniciar tot el procés de negociació començant un altre cop pel *DHCP discovery*.

DHCP 'decline'

Per la seva part, el client també pot examinar l'adreça IP oferta pel servidor per comprovar si està en ús o no. Pot fer altres proves per veure si li sembla correcta o no l'oferta rebuda del servidor. Per exemple, en el cas de renovació d'una adreça IP, el client pot rebre una IP diferent a la que utilitza i no interessar-li. En aquests casos, el client pot enviar un paquet *DHCP decline* al servidor per indicar que la seva oferta ha estat rebutjada.

2.2.3 DHCP 'release'

Quan un client ja no necessita més l'ús de la configuració IP que ha rebut, la pot alliberar enviant al servidor un paquet *DHCP release*. En fer-ho, el servidor afegeix l'adreça IP al conjunt d'adreces dinàmiques que té disponibles. També fa l'anotació pertinent en el registre de concessions (*leases*) per indicar que ha finalitzat l'ús de l'adreça. De totes maneres, molt sovint el client no pot arribar a emetre aquest paquet perquè és apagat per l'usuari sense deixar temps al sistema per alliberar la IP.

DHCP 'information'

En qualsevol moment el client pot sol·licitar més informació sobre la configuració de xarxa al servidor utilitzant un paquet *DHCP information*. En el paquet DHCP *offer* que el servidor envia al client, consten les informacions generals de configuració de xarxa que es trameten en l'oferta: adreça IP, màscara de xarxa, porta d'enllaç predeterminada, servidor DNS, fitxer a baixar per a arrencades PXE i molts altres paràmetres que poden estar configurats per enviar-se en l'oferta. El client pot tornar a demanar al servidor la informació d'aquests paràmetres o pot sol·licitar informació per a la configuració d'altres paràmetres (WINS, NetBIOS, *hostname*...). El client només pot realitzar una petició d'informació *DHCP information* al servidor un cop està configurat.

Petició de renovació/concessió d'una IP concreta

El procés de quatre fases usuals de DHCP consistent en *discovery* / *offer* / *request* / *ack* es produeix quan el client sol·licita una adreça IP de nou. Sabem que les concessions són per un interval de temps finit, passat el qual cal que el client en demani la renovació. Existeix, doncs, un procés de renovació simplificat. El client demana continuar usant la mateixa adreça IP amb un paquet DHCP *request* i el servidor li concedeix o no amb els paquets DHCP ACK/NACK.

Un altre cas és un client que demana usar (renovar) una adreça IP que el servidor no li pot concedir (està en ús, no és del rang que gestiona...). En aquesta situació, el servidor envia un DHCP NACK.

Macchanger

Aquesta ordre GNU/Linux permet emmascarar l'adreça MAC pròpia (*mascarade*), simular que és una altra.

2.2.4 Atacs al funcionament del DHCP

Com qualsevol altre servei de xarxa, el servidor DHCP és susceptible de patir atacs malintencionats. L'atac més fàcil i clàssic és el DoS o denegació de servei. Consisteix a inundar de peticions un servidor per tal de saturar-lo i bloquejar-ne el funcionament. Un client pot realitzar innumerables peticions *DHCP discovery* fingint que són clients diferents (emmascarant la seva MAC) amb la intenció d'esgotar les adreces IP disponibles del servidor o simplement amb la intenció de sobrecarregar-lo amb tantes peticions que no doni a l'abast a atendre-les o que ho faci lentament.

Un altre tipus d'atac consisteix a falsejar la informació que s'envia al client. Recordeu que el client fa una sol·licitud d'IP en forma de difusió (*broadcast*) i la seva petició pot ser atesa per un o més servidors DHCP. Un dels servidors DHCP pot ser un atacant que intenta proporcionar informació de configuració falsa al client, per exemple, indicant un servidor DNS també maliciós. Aquest pot falsejar les identitats de les màquines de la xarxa i que quan el client s'adreci a la seva entitat bancària el servidor DNS en realitat li proporcioni una IP d'una màquina que falseja la de l'entitat bancària.

Tipus d'atacs DNS

- Clients no autoritzats: accés a servidors DNS per part de clients no autoritzats.
- Servidors no autoritzats: servidors DNS impostors que suplanten els vertaders servidors.

Per posar remei a la inseguretat en la comunicació client/servidor DHCP, el protocol permet utilitzar mecanismes d'autenticació i xifratge. Aquests mecanismes queden fora de l'abast d'aquesta explicació.

2.2.5 Conflictes amb les adreces IP

Un dels principals motius per utilitzar DHCP és simplificar el procés de configuració de xarxa i minimitzar els conflictes per encavalcament d'adreces IP. Per desgràcia, això no garanteix que no es puguin produir conflictes. Per exemple, ens podem trobar en situacions en què dues màquines diferents tinguin la mateixa IP per una simple mala configuració del servidor DHCP. Un altre cas típic és el d'un client que s'ha configurat ell mateix una IP estàtica quan en la xarxa ja hi havia un equip que utilitzava la mateixa adreça IP assignada pel servidor DHCP.

Un problema habitual per als administradors poc experimentats és definir una configuració de xarxa local al client (*hostname*, servidor DNS, porta d'enllaç a utilitzar...), però demanar l'adreça IP dinàmicament. La configuració dinàmica no és solament la IP i la màscara sinó que el servidor DHCP pot proporcionar altres paràmetres de xarxa que sobreescriuran els que el client tenia definits localment (aquest és l'objectiu del DHCP!).

La configuració rebuda per DHCP sobreescriu la configuració local del client.

2.2.6 Rangs i concessions

Els clients DHCP obtenen del servidor una configuració de xarxa. Descrivim ara alguns dels termes que apareixen en aquest procés i que formen part de la configuració DHCP.

- **Rang**: anomenen *rang d'adreces IP* el conjunt d'adreces dinàmiques que el servidor té disponibles per assignar als clients. Les adreces IP disponibles s'agrupen per oferir-se a les diverses subxarxes que atén el servidor. Una mateixa subxarxa pot disposar de diversos rangs. Segurament s'entendrà més fàcilment amb un exemple:

```
subnet 140.220.191.0 netmask 255.255.255.0 {
            range 140.220.191.150 239.252.197.250;
}

subnet 239.252.197.0 netmask 255.255.255.0 {
            range 239.252.197.10 239.252.197.107;
            range 239.252.197.113 239.252.197.250;
}
```

En l'exemple anterior s'observa que la primera subxarxa disposa d'un rang de 101 adreces dinàmiques (de la 140.220.191.150 a la 250). La segona subxarxa permet assignar dinàmicament dos rangs d'adreces no correlatius.

- **Exclusions**: entenem per *exclusions* aquelles adreces IP que no s'ofereixen dinàmicament per part del servidor. És a dir, que no formen part de cap rang.

- **Concessions**: l'assignació d'una adreça IP i la resta de paràmetres de xarxa a un client per part del servidor és una concessió o *lease*. Els clients reben les concessions per períodes de temps finits que, en finalitzar, cal renegociar. Tant el client com el servidor s'anoten les concessions, el client la que rep i el servidor les que concedeix. Quan finalitza una concessió, el servidor pot decidir revocar-la o ampliar-la.

El client pot decidir renunciar a la concessió en qualsevol moment. Si el client vol allargar la concessió inicia un diàleg DHCP abreujat amb el servidor que pot acabar amb una renovació o amb la pèrdua de la concessió (sempre pot tornar a començar el procés). Tant el servidor com el client miren normalment les concessions que s'han efectuat entre ells amb anterioritat per tal de, si és possible, repetir la mateixa assignació.

Alliberament d'una concessió

El client pot alliberar (*release* en anglès) una concessió directament des de la línia de comandes. En un entorn Linux:

dhclient -r

En un entorn Windows:

ipconfig /release

- **Reserves**: anomenem *reserves* aquelles adreces IP que s'assignen per DHCP però de manera fixa. És a dir, són adreces que s'assignen dinàmicament però sempre i únicament a un *host* determinat. Fixeu-vos que tot i ser una adreça dinàmica només s'utilitza si el *host* associat en fa ús. Si el *host* està apagat, l'adreça no es pot usar per a altres *hosts*, està reservada. Un exemple de reserva podria ser:

```
subnet 140.220.191.0 netmask 255.255.255.0 {
       host iocserver {
           hardware ethernet 08:00:2b:4c:59:23;
           fixed-address 140.220.191.1;
       }
      range 140.220.191.150 239.252.197.250;
       }
```

En aquest exemple es pot veure que l'adreça 140.220.191.1 és una adreça reservada exclusivament per al *host* iocserver, que s'identifica mitjançant la seva adreça MAC.

2.2.7 DHCP, un servei client/servidor

Com acostuma a passar amb els serveis client/servidor, un equip pot realitzar les dues funcions al mateix temps.

El servei DHCP és un més dels serveis de xarxa que tenen l'estructura client/-servidor. Els servidors DHCP són els equips que tenen en execució el programa servidor. És el programa encarregat d'atendre les peticions dels clients i oferir-los la configuració de xarxa, tot portant el registre de les IP que concedeix i de totes les accions que realitza. Els clients DHCP són aquells equips que realitzen peticions a un servidor DHCP per obtenir una configuració de xarxa.

ISP

ISP: *Internet service provider* o proveïdor de servei/accés a Internet. Ho són, per exemple, les empreses Ono, Vodafone o Jazztel.

Client DHCP

Un equip client DHCP és un equip que sol·licita l'adreça IP i altres paràmetres de configuració de xarxa a un servidor DHCP en lloc de tenir-los definits localment en l'equip.

Si connecteu el vostre equip informàtic a la xarxa Internet per mitjà d'un ISP (*Internet service provider* o proveïdor d'accés a Internet), segurament rebreu una IP dinàmica del vostre proveïdor. Quan es realitzava una trucada telefònica amb mòdem i usant el protocol PPP (Point to Point Protocol o protocol punt a punt), el proveïdor proporcionava una adreça IP dinàmica. Si utilitzeu ADSL i un encaminador o *router*, segurament l'encaminador us proporciona una adreça IP dinàmica privada a l'ordinador de casa. Al mateix temps, l'encaminador obté una adreça IP dinàmica pública del proveïdor. Aquestes adreces IP dinàmiques són fixes (sempre les mateixes) o dinàmiques de rang (pot ser qualsevol adreça IP del conjunt d'adreces IP que té disponibles per concedir el servidor DHCP).

L'encaminador: servidor i client DHCP

Un cas típic en una xarxa privada a casa és disposar d'un encaminador ADSL connectat a un proveïdor ISP. L'encaminador actua com a client DHCP en la seva interfície de xarxa pública (la de l'ADSL), la que connecta a Internet.

Alhora, l'encaminador fa usualment de servidor DHCP per als ordinadors de casa proporcionant-los una adreça IP. En general els ordinadors dels usuaris es configuren com a clients DHCP.

IP pública / IP privada

La diferència entre una IP pública i una IP privada és que la pública és visible per a tots els equips d'Internet, mentre que la privada és visible només dins de la mateixa xarxa local.

El client DHCP ha de tenir en funcionament un dimoni encarregat de la gestió de les tasques DHCP pròpies del client. Realitza la part de negociació encarregada al client (*DHCP discovery*, *request*) i també porta un registre de les concessions (*leases*) rebudes. Aquest registre és el que utilitza el client per tornar a demanar la mateixa IP que tenia anteriorment. Un cop rebuda la concessió, el programa client queda "adormit", pendent de tornar-se a executar automàticament quan calgui renegociar la concessió. Sense intervenció de l'usuari, el programa client s'activa i segueix el procediment necessari per renegociar l'adreça IP cada cop que el temps de la concessió s'exhaureix.

Configuració client

Usualment, les configuracions client es poden fer de tres maneres diferents:

- Fitxer de text: editar directament els fitxers de configuració.
- Menús en mode text: usant algun programa de menús amb interfície de text.
- Aplicació gràfica: usant una aplicació de finestres en l'entorn gràfic.

Els programes client varien d'un sistema operatiu a un altre i la manera d'executar-los també. Generalment es disposa d'un client executable en mode text o ordres i d'una interfície gràfica (GUI, *graphics user interface* o interfície gràfica d'usuari) per a la configuració. No cal dir que els sistemes Windows tendeixen a la configuració gràfica usant finestres i a la configuració i execució interna d'amagat de l'usuari. Normalment, en els sistemes GNU/Linux la configuració es fa usant fitxers de text o opcions que es donen a ordres executables. La interfície gràfica acostuma a ser un *frontend* per cridar l'ordre. Segons sigui el sistema operatiu es pot consultar el fitxer de registre de les concessions rebudes pel client, el fitxer de *leases*, més o menys detalladament.

'Frontend'

Part que està formada per una interfície gràfica i que acostuma a recollir dades interactuant amb l'usuari. És molt comú en els entorns Unix/Linux tenir comandes molt potents amb una varietat d'opcions i disposar d'algun *frontend* per a aquella comanda perquè la interacció sigui més amigable.

Generalment, el programa client es pot configurar per definir com es comunicarà amb el servidor: informació a demanar, informació a proporcionar al servidor, opcions per defecte...

Servidor DHCP

L'administrador de xarxa és l'encarregat de pensar la ubicació del servidor o servidors DHCP en l'estructura corporativa. Com més complicada sigui la topologia de la xarxa, més difícil en serà la gestió. Una xarxa corporativa bàsica pot disposar d'un únic servidor DHCP que ofereix els seus serveis a tots els equips de la xarxa. Els clients poden estar en una mateixa subxarxa o en diverses subxarxes, però totes amb connectivitat amb el servidor DHCP. Aquest també pot ser l'esquema d'una xarxa privada a casa, on un encaminador (el de l'ISP, per exemple) proporciona el servei DHCP a tots els ordinadors de la casa.

Si la xarxa corporativa creix i passa a tenir subxarxes segmentades amb tallafocs, la configuració del servidor DHCP es complica. Si es vol continuar disposant d'un únic servidor per a tota la xarxa, caldrà que els tallafocs (*firewalls*) deixin passar els paquets DHCP entre les subxarxes i el servidor. Una altra opció és posar un servidor DHCP per a cada subxarxa o grups de subxarxes. Fent-ho així, l'administració de cada servidor és més senzilla, però hi ha més servidors a administrar. Una xarxa amb una casuística completa és la que té diversos servidors DHCP per a diverses parts de la xarxa i tallafocs entre clients i servidors que han de permetre el pas de paquets DHCP.

Si el servidor DHCP és l'encarregat de donar adreces IP als clients, qui li proporciona una adreça IP a ell? Ho fa o bé un altre servidor DHCP (i podríem tornar a fer la mateixa pregunta indefinidament) o bé l'administrador. Usualment, en una xarxa corporativa el servidor DHCP utilitza una IP estàtica definida per l'administrador. Això li permet estar sempre disponible per als clients amb la mateixa IP i no el fa dependre d'un servidor extern.

Hi ha diversos programes servidors DHCP que es poden classificar en dos grans grups: els que treballen en mode text i els que ho fan en mode gràfic. Cada administrador treballa amb les seves eines preferides. Les tasques bàsiques per aprendre a utilitzar un servidor DHCP són: observar, fer una llista de la configuració actual, activar/aturar el servei, modificar la configuració, monitorar els *logs* (registre de successos del servei) i, evidentment, saber instal·lar i desinstal·lar l'aplicació servidor.

Els fitxers de *logs* (successos) recullen els esdeveniments que es volen monitorar.

Com la majoria de serveis de xarxa, el servei DHCP s'executa en segon pla en forma de dimoni. El servidor DHCP sempre està engegat escoltant en el port 67 les peticions que rep dels clients. Quan rep una petició entrant, el programa executable del servidor DHCP la processa i posa en marxa tot el mecanisme DHCP pertinent per tornar a escoltar noves peticions. De fet, el servidor sempre escolta peticions i les processa simultàniament (segons la configuració).

Els fitxers del registre del servei, on s'anoten les concessions, mantenen la informació encara que el servei s'aturi o que el servidor s'apagui. En tornar a engegar-lo es llegiran de nou els fitxers de registres per tal de saber quines són les concessions que s'havien realitzat.

Els fitxers de concessions permeten mantenir la coherència de l'assignació d'adreces IP entre aturades del servei.

2.3 Instal·lació del servidor DHCP

El servei de xarxa DHCP està estructurat en forma de servei client/servidor; per tant, caldrà disposar del programari apropiat per interpretar cada un d'aquests rols. El programari que fa la funció de client ja està usualment integrat en el sistema operatiu. És a dir, per disposar de la part client del servei DHCP normalment no cal instal·lar res.

Així, doncs, quan parlem d'instal·lar un servei DHCP fem referència al procés d'instal·lació i configuració del programari del servidor DHCP. Evidentment també caldrà configurar els clients adequadament per fer ús del servei.

La instal·lació del programari que proporciona el servei DHCP es fa de manera molt similar (per no dir idèntica) al programari d'altres serveis de xarxa com DNS, HTTP o FTP. Es tracta d'instal·lar el programari de l'aplicació servidor i fer-ne la configuració apropiada.

Per fer-ho cal fer les reflexions i els passos següents:

1. Preguntarse: Quin programari proporciona aquest servei? Quines característiques té? Com es pot adquirir?
2. Obtenir l'aplicació que proporciona el servei DHCP.
3. Observar l'estat de la xarxa actual. Està ja el servei en funcionament? Existeix ja una configuració DHCP activa?
4. Instal·lar l'aplicació servidor.
5. Comprovar que la instal·lació s'ha fet correctament.
6. Configurar el servei en el servidor i activar els clients perquè l'utilitzin.
7. Comprovar que el servei funciona correctament.

2.3.1 Aplicacions servidor DHCP

Sempre que l'administrador vol posar en funcionament un nou servei de xarxa cal que primerament analitzi quines aplicacions hi ha al mercat que ofereixen aquest servei. És feina seva estudiar les característiques de les diverses aplicacions, avaluar-ne l'eficiència, el cost, el que en diuen altres usuaris... La manera més fàcil de fer això és navegar per Internet, consultar les revistes especialitzades o demanar consell a informàtics experts.

Usualment, però, l'administrador acaba utilitzant l'aplicació servidor DHCP que li proporciona el mateix sistema operatiu. Si utilitzeu Windows, l'empresa Microsoft disposa d'una aplicació pròpia, però també en podeu trobar d'altres a

Internet. Igualment, si utilitzeu GNU/Linux segurament la mateixa distribució ja proporciona un servidor DHCP. De totes maneres també en podeu obtenir d'altres a Internet.

2.4 Configuració del servei

Per configurar el servei DHCP primer cal saber observar i manipular la configuració de xarxa existent, i això consisteix a:

- Fer la llista de la configuració de xarxa actual.
- Comprovar l'estat del servei de xarxa.
- Activar/desactivar el servei de xarxa.
- Monitorar el servei i el procés del servidor.

Les tasques principals per configurar un servidor DHCP són les següents:

Exemples de configuració

A GNU/Linux és molt usual que el paquet que proporciona un servei inclogui un fitxer d'exemple de configuració. El servei DHCP inclou el fitxer dhcpd.conf i la pàgina de manual del mateix nom.

- Instal·lar el programari del servidor DHCP.
- Activar/desactivar el servei del DHCP.
- Fer la llista de la configuració actual del servidor DHCP.
- Modificar la configuració del servidor DHCP.
- Monitorar els *logs* del servei DHCP i els fitxers de registre de les concessions (*leases*).

Abans d'endinsar-nos en la configuració del servei és molt útil observar una configuració ja existent. Un exemple de fitxer de configuració del servei DHCP és el que es mostra a continuació:

```
# a) opcions globals del servidor DHCP (usuals)
ddns-update-style interim;
ignore client-updates;

# b) definició de la xarxa a la qual s'ofereix el servei DHCP
subnet 192.168.0.0 netmask 255.255.255.0 {
   # opcions genèriques per a tots els equips de la xarxa
   option routers      192.168.0.1;
   option subnet-mask     255.255.255.0;
   option domain-name     "domain.org";
   option domain-name-servers  192.168.1.1;

   # definició del rang d'IP dinàmiques a usar
   # i dels temps de les concessions
   range dynamic-bootp 192.168.0.128 192.168.0.254;
   default-lease-time 21600;
   max-lease-time 43200;

  # c) opcions d'equips individuals
  # el servidor NS obté sempre una adreça fixa basada en MAC
```

```
  host ns {
   next-server marvin.redhat.com;
   hardware ethernet 12:34:56:78:AB:CD;
   fixed-address 207.175.42.254;
  }
}
```

En aquest fitxer de configuració es pot veure que hi ha tres àmbits diferents de definició:

1. **Opcions globals del servidor DHCP**. Són opcions que indiquen al servidor la manera d'actuar. També són opcions generals que cal aplicar a totes les concessions que es realitzin, independentment de la xarxa o equip.

2. **Definicions i opcions de xarxa**. Es defineixen tantes (sub)xarxes com atén el servidor. Cada definició de subxarxa consta de l'adreça IP de la xarxa i la màscara corresponent. Entre claus s'indiquen totes les opcions específiques per a les concessions de les adreces IP corresponents a la subxarxa. És habitual indicar el rang o *pool* d'adreces dinàmiques a usar, la porta d'enllaç predeterminada, el servidor de noms...

3. **Opcions d'equips individuals**. Dins d'una subxarxa es poden definir opcions per a equips individuals. Cal identificar els equips per la seva adreça MAC i, entre claus, indicar les opcions que els són específiques. Això permet assignar adreces fixes dinàmicament (equivalent al protocol BOOTP) usant les opcions de maquinari Ethernet i *fixed-address*.

Les opcions globals de configuració DHCP es poden redefinir amb valors diferents dins d'un bloc de xarxa concret. Dins d'un equip també es poden definir opcions amb valors diferents als definits per a la xarxa o globalment. Tal com passa en els llenguatges de programació, preval el valor més intern, el de *host* per damunt del de xarxa i el de xarxa per damunt del global.

2.4.1 Configuració bàsica

Per fer funcionar el servidor DHCP cal configurar-lo. Per poder arrencar li cal saber a quina xarxa donarà servei i quin és el rang d'adreces IP que pot usar dinàmicament per a les concessions als clients.

El paquet DHCP conté un fitxer d'exemple al directori /user/share/doc/dhcp*/dhcpd.conf.sample. Aquest fitxer es pot copiar a /etc/dhcpd.conf i passarà a ser la configuració bàsica del servidor DHCP. Podem veure'n el contingut fent:

```
root@server:~# ls -l /usr/share/doc/isc-dhcp-server/examples/dhcpd.conf.example
-rw-r--r-- 1 root root 3496 de des.  11  2018 /usr/share/doc/isc-dhcp-server/
    examples/dhcpd.conf.example
root@server:~# head /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
```

```
8
9  # option definitions common to all supported networks...
10 option domain-name "example.org";
11 option domain-name-servers ns1.example.org, ns2.example.org;
12
13 default-lease-time 600;
14 root@server:~#
```

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

- Opcions globals: indiquen al servidor que ignori les actualitzacions dels clients i el tipus de DDNS a usar (actualitzacions dinàmiques de DNS).
- Definició de subxarxa: cal definir tants blocs de subxarxa com subxarxes atengui el servidor DHCP.
- Opcions genèriques de subxarxa: es poden indicar opcions genèriques per als equips d'una subxarxa. Evidentment poden diferir de les opcions d'altres subxarxes.
- Les opcions principals de xarxa a descriure són l'encaminador, la màscara de xarxa, el domini...
- Les opcions principals a descriure del servei DHCP són el rang d'adreces IP dinàmiques a usar i el temps màxim de concessió.
- Perquè un *host* determinat tingui sempre la mateixa adreça IP es poden fer entrades individualitzades per a *hosts* concrets. Els *hosts* s'identifiquen per la seva adreça MAC.
- A un *host* concret se li poden aplicar opcions individualitzades, com per exemple definir el seu nom. Les opcions individuals prevalen sobre les genèriques.

2.4.2 Configuració avançada

El protocol DHCP permet configuracions d'una certa complexitat. Podeu consultar la documentació del DHCP i les pàgines del manual sobre el dimoni dhcpd i el fitxer de configuració dhcpd.conf.

Les característiques principals que s'hi descriuen són l'agrupació d'entrades en grups i classes i la possibilitat que el DHCP es comuniqui amb el DNS (actualitzacions DDNS) per crear entrades DNS quan un equip rep una configuració DHCP.

Vegeu un exemple de configuració amb opcions més avançades:

```
1  # option definitions common to all supported networks...
2  option domain-name "example.org";
3  option domain-name-servers ns1.example.org, ns2.example.org;
4
5  default-lease-time 600;
```

```
max-lease-time 7200;

ddns-update-style none;
authoritative;

subnet 10.5.5.0 netmask 255.255.255.224 {
  range 10.5.5.26 10.5.5.30;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;
  max-lease-time 7200;
}

host fantasia {
  hardware ethernet 08:00:07:26:c0:a5;
  fixed-address fantasia.example.com;
}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

class "foo" {
  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
}

shared-network 224-29 {
  subnet 10.17.224.0 netmask 255.255.255.0 {
    option routers rtr-224.example.org;
  }
  subnet 10.0.29.0 netmask 255.255.255.0 {
    option routers rtr-29.example.org;
  }
  pool {
    allow members of "foo";
    range 10.17.224.10 10.17.224.250;
  }
  pool {
    deny members of "foo";
    range 10.0.29.10 10.0.29.230;
  }
}
```

Base de dades de concessions fetes pel servidor

El servidor desa en una base de dades local (de fet, són fitxers de text) les concessions (*leases*) que realitza. D'aquesta manera en pot seguir la pista en tot moment. Generalment les té a la memòria (per permetre'n un accés més ràpid), però en manté una còpia al disc. Si, per exemple, el sistema o el servei es reinicia, pot saber quines són les concessions que encara estan actives (i, per tant, quines adreces IP no té disponibles).

Usualment el fitxer de concessions és a /var/lib/dhcp. Vegeu-ne el contingut fent:

```
root@server:~# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

root@server:~#
```

2.5 Assignacions estàtiques i dinàmiques

Els clients de xarxa o bé tenen una configuració estàtica on es defineixen els seus paràmetres o bé reben la configuració per DHCP. El procés de configurar un client DHCP és tan senzill com activar aquesta última opció usant algun dels mètodes adients.

La configuració dels clients DHCP consisteix en el següent:

- Observar la configuració de xarxa actual del client.
- Configurar el client per rebre dinàmicament una adreça IP. Es tracta d'activar/desactivar la configuració de xarxa dinàmica o estàtica.
- Sol·licitar una nova IP al servidor DHCP.
- Fer la llista del fitxer de registre de les concessions client rebudes.
- Activar/desactivar el servei de xarxa en el client.

2.5.1 Client dinàmic

Tot equip client de xarxa necessita una configuració apropiada. Si aquesta configuració es defineix element per element en el mateix equip, s'anomena configuració estàtica. Si és així, no cal un servidor DHCP. És quan els clients reben la configuració de xarxa externament que parlem de configuració dinàmica i ens cal un servidor DHCP que la proporcioni.

La configuració del client es pot fer en mode text editant directament els fitxers, utilitzant interfícies de text o gràfiques (*applets*).

Edició dels fitxers de configuració

Es pot editar directament el fitxer de configuració de la interfície de xarxa pertinent i establir l'opció *dhcp* a la directiva *iface* per activar el client DHCP. Si per exemple es vol configurar la interfície de xarxa *enp0s3*, el fitxer hauria de tenir el següent aspecte:

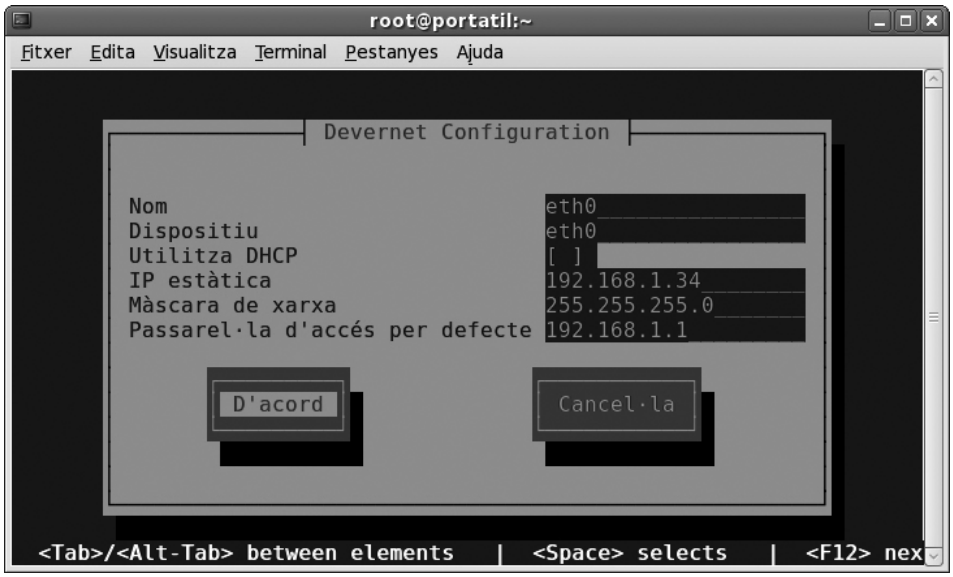
```
root@server:~# cat /etc/network/interfaces
auto lo
iface lo inet loopback
auto enp0s3
iface enp0s3 inet dhcp
root@server:~#
```

Menús amb interfície de text

Un altre mecanisme per activar el client DHCP és utilitzar alguna utilitat de menús en entorn de text (varien segons el sistema i se'n poden trobar a Internet), tot i que estan en força desús.

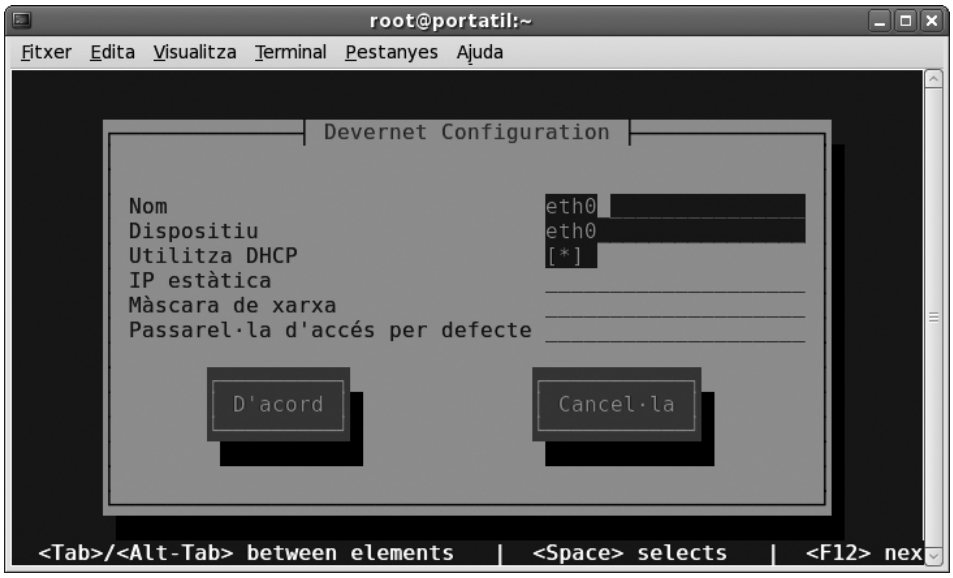
La figura 2.2 que mostra una configuració de client de xarxa estàtica i on es pot veure que la casella que permet activar el client DHCP està desactivada.

Figura 2.2. Configuració estàtica del client DHCP



El procediment per activar el client de xarxa DHCP és molt senzill. N'hi ha prou d'activar l'opció pertinent, tal com mostra la figura 2.3 ("Activació del client DHCP usant menús de text").

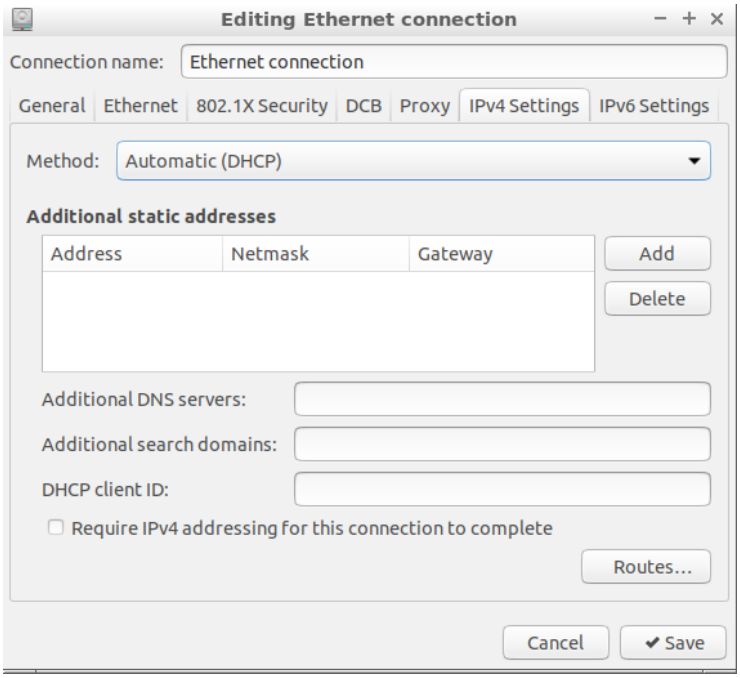
Figura 2.3. Activació del client DHCP usant menús de text



Menús en mode gràfic

En mode gràfic, el sistema també proporciona mecanismes per configurar les interfícies de xarxa i establir el mode d'activació a DHCP. En la figura 2.4 es pot observar que la configuració de la interfície té activada l'opció de configuració de xarxa per DHCP.

FIGURA 2.4. Activació del client DHCP usant l'entorn gràfic



2.5.2 Renovació de l'adreça IP

El client DHCP pot alliberar l'adreça que utilitza quan ho creu pertinent. En fer-ho, el servidor anota la fi de la concessió i si es tracta d'una adreça dinàmica de rang torna a quedar disponible per assignar-la a un altre client. Quan a un client se li està acabant el temps de concessió ha de tornar a negociar una adreça amb el servidor. De totes maneres, si el client vol, en pot tornar a sol·licitar una en qualsevol moment.

El client pot alliberar una adreça (*release*) que està en ús en qualsevol moment. Pot forçar-ho fent, per exemple:

```
root@client:~# dhclient -r -v enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:f8:f9:29
Sending on   LPF/enp0s3/08:00:27:f8:f9:29
Sending on   Socket/fallback
DHCPRELEASE on enp0s3 to 10.0.2.3 port 67 (xid=0x3ab21a2a)
```

Per forçar el client a demanar una nova adreça per a la interfície Ethernet *enp0s3* es pot fer:

```
root@client:~# dhclient  -v enp0s3
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:f8:f9:29
Sending on   LPF/enp0s3/08:00:27:f8:f9:29
Sending on   Socket/fallback
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0xf5a1913d)
DHCPREQUEST of 10.0.2.10 on enp0s3 to 255.255.255.255 port 67 (xid=0x3d91a1f5)
DHCPOFFER of 10.0.2.10 from 10.0.2.3
DHCPACK of 10.0.2.10 from 10.0.2.3
bound to 10.0.2.10 -- renewal in 506 seconds.
```

La comanda *dhclient* amb el paràmetre -v (*verbose*) és molt útil ja que mostra molta informació, i en cas d'error (mala configuració, error de xarxa, etc.) permet afinar molt d'on prové l'error.

2.5.3 Registre de concessions rebudes

El client DHCP porta un registre de les concessions rebudes; d'aquesta manera pot tornar a demanar una concessió abans que expiri l'actual. Aquest registre també serveix per demanar al servidor una adreça IP concreta. Les concessions o *leases* del client es desen en un fitxer anomenat /var/lib/dhcp/dhclient.leases. Podem veure'n el contingut fent:

```
root@client:~# tail /var/lib/dhcp/dhclient.leases
  option subnet-mask 255.255.255.0;
  option routers 10.0.2.1;
  option dhcp-lease-time 1200;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 10.0.2.3;
  renew 6 2020/07/11 14:20:25;
  rebind 6 2020/07/11 14:28:39;
  expire 6 2020/07/11 14:31:09;
}
root@client:~#
```

En l'apartat "Funcionament del protocol DHCP" podeu observar detalladament com és el diàleg entre el client i el servidor.

En l'apartat "Renovar l'adreça IP" s'explica com forçar el client a demanar una nova configuració.

Podeu manipular vosaltres mateixos la captura del trànsit de xarxa DNS carregant el fitxer de captura del Wireshark que es lliura com a material complementari. Aquest fitxer el trobareu en la secció "Annexos" del web del mòdul.

2.5.4 Comprovació del funcionament

La millor manera de comprovar el funcionament del DHCP és simplement posant-lo en marxa, és a dir, creant una xarxa amb diversos clients DHCP i un servidor que els atengui. Per saber si el servei funciona cal mirar un per un cada client i comprovar que han rebut la configuració de xarxa correcta. El problema, però, és què fer si els clients no es configuren correctament.

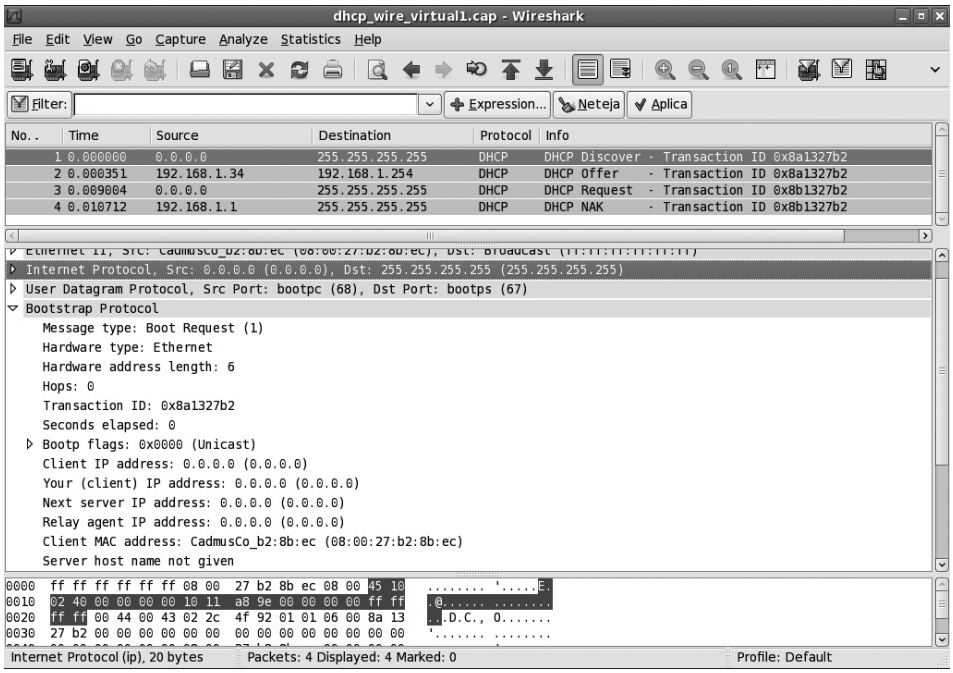
Els passos més usuals a seguir per a la resolució de problemes són:

- Comprovar que la xarxa està correctament connectada físicament, és a dir, cables, connectors, interfícies...
- Mirar si existeix connectivitat entre els equips, per exemple, usant una configuració estàtica. Això permetrà descartar que els problemes siguin deguts a altres causes. Si el DHCP no va és que no està configurat correctament.
- Repassar la configuració del client i del servidor DHCP, especialment la del servidor. Es pot començar fent la configuració tan senzilla com sigui possible. Un cop funciona es pot anar avançant en la seva complexitat.
- Examinar els fitxers de concessions, tant el del client com el del servidor, per detectar-hi anomalies.
- Quan la comunicació client/servidor no funciona correctament i no sabem per què, és molt útil monitorar el trànsit de xarxa mitjançant alguna eina d'anàlisi dels paquets que viatgen per la xarxa.

Centrem-nos, doncs, en el monitoratge del trànsit de xarxa per tal de comprovar que el diàleg entre el client i el servidor és l'apropiat. Existeixen moltes eines al mercat (que podeu trobar per Internet) que fan aquesta funció. Una de les més recomanables és Wireshark. Amb aquesta aplicació hem de poder observar l'intercanvi dels paquets *DHCP discover*, *DHCP offer*, *DHCP request* i *DHCP ack* que es produeix quan tot el procés DHCP funciona correctament. Si aquest intercanvi no es produeix és que hi ha algun problema.

En la figura 2.5 ("Captura d'un diàleg DHCP client/servidor") podeu observar una captura de trànsit DHCP feta amb Wireshark. La captura s'ha fet al servidor i s'ha forçat al client a demanar de nou una configuració de xarxa amb la utilitat *dhclient*.

Figura 2.5. Captura d'un diàleg DHCP client



servidor

2.6 Opcions addicionals de configuració

Com en la majoria de serveis actuals, la quantitat d'opcions de configuració és impressionant, per no dir aterridora. L'administrador de xarxa ha de conèixer les opcions bàsiques per configurar el servei DHCP, que inclouen l'assignació d'una configuració de xarxa bàsica, els temps de les concessions, assignacions dinàmiques i fixes, i fitxers d'arrencada via PXE.

Existeixen centenars d'opcions de configuració que permeten especificar la configuració del client fins al mínimin detall. Més important encara, existeixen diversos mecanismes per agrupar les opcions per *host*, subxarxa, classe, *pool*..., fet que premet definir "prototipus" de configuració per aplicar a *hosts* segons si tenen o no unes característiques determinades.

També existeixen extensions DHCP que permeten usar expressions i llenguatges de programació per poder realitzar configuracions complexes que permeten decidir quin tipus de configuració assignar al client.

2.6.1 Opcions de configuració del servidor i àmbit d'aplicació

Les opcions de configuració DHCP són múltiples i comprenen molts àmbits. Algunes permeten la compatibilitat amb sistemes antics, d'altres, amb altres tipus de xarxes... No és imaginable que un administrador de xarxes les conegui totes a fons. Normalment fa ús d'un conjunt reduït d'opcions que és més que suficient per administrar la majoria de xarxes.

La configuració DHCP es pot definir tant en el client com en el servidor, tot i que usualment es fa en el servidor. La tasca principal és configurar un servidor per tal de proporcionar les opcions apropiades a cada subxarxa. De totes maneres, però, un client també pot disposar d'un fitxer de configuració en el qual es defineixen quins són els seus requeriments i com ha de ser el diàleg amb el servidor. Per exemple, es defineixen quines opcions ha de sol·licitar, valors per defecte de determinades opcions (per si el servidor no en proporciona). El client també pot definir informació que proporcionarà al servidor per tal que aquest prengui decisions dinàmicament.

Caldrà, doncs, entendre quins són els àmbits (*scope*) de definició de sentències i opcions, com s'agrupen les subxarxes i els *hosts*, quines són les opcions globals, com es realitzen les definicions condicionals i molts altres detalls.

Àmbit de definició

Els clients es poden agrupar en diversos àmbits per tal de definir les opcions que han de rebre. El mateix servidor DHCP pot actuar de manera diferent segons quin

sigui l'àmbit de definició.

Alguns dels conceptes a tractar són:

- *Subnets*
- Període de concessió
- Adreces fixes o reservades: identificació de *hosts*
- PXE: protocol d'arrencada via xarxa
- Àmbit d'aplicació
- *Pool*

Les sentències d'àmbit d'aplicació més usuals són *subnet* i *host*, que permeten identificar una subxarxa i un host concret respectivament. Les subxarxes es poden agrupar en *shared-network* i els clients es poden agrupar usant la sentència ***group***. Les opcions es poden definir en funció de determinats requisits que compleixi el client mitjançant la sentència ***class*** i les **declaracions condicionals**.

El servei DHCP es pot configurar amb multitud de sentències que es poden repassar a l'RFC 2131 i a la pàgina de manual dhcpd.conf(5). Els clients DHCP reben del servidor la configuració de xarxa. Usualment parlem de l'adreça IP i la màscara, però de fet poden rebre gran quantitat de paràmetres de configuració de xarxa i informació sobre diversos serveis de xarxa disponibles. El client, per la seva part, pot sol·licitar paràmetres concrets al servidor. Quan configura el servei DHCP, l'administrador de xarxa no ha d'especificar totes les opcions possibles (de fet són moltíssimes), sinó només les que siguin necessàries per a cada client. Algunes opcions prenen valors per defecte i no cal especificar-les, d'altres no poden ser alterades pel servidor.

Una de les possibilitats que ofereix el DHCP és configurar les opcions de xarxa en funció de qui i de com és el client. És a dir, assignar al client una configuració de xarxa o una altra en funció de la informació que proporciona. Fixeu-vos que no es tracta d'entrades *host* estàtiques per a cada client, sinó que un mateix client tindrà una o altra configuració segons la informació que proporcioni.

2.7 Documentació de procediments

Una de les feines més desconegudes en el món de la informàtica és la confecció de manuals i documentació de suport. Com a clients, molt sovint ens queixem que ens falta informació o que està mal redactada. Com a administradors de xarxa, en canvi, no trobem mai temps per anotar les coses. Mentre les tenim al cap no creiem necessari fer la documentació, i després ja ens és impossible fer-ho, i sovint és just quan ens faria falta haver-ho fet.

Cal tenir clara la informació que cal documentar, tant per a l'usuari com per a l'administrador.

El client ha de saber:

- Com contactar amb el servidor DHCP. Quin programari ha d'utilitzar i com l'ha de configurar per fer ús del servei.
- Quina és la informació que obtindrà via DHCP. Cal saber consultar aquesta informació i saber què significa, per a què serveix.

La documentació de l'usuari ha de descriure el procés per activar el client DHCP, amb l'ajut de captures de pantalla. Calen també exemples de llista de concessions rebudes: on són i com es poden consultar. La part més important és mostrar un exemple de configuració de xarxa rebuda en el qual es detalli el significat de cada element i explicar a l'usuari com fer aquesta consulta.