

## **A) Servei DNS**

És un servei que té com a funció principal realitzar l'assignació i traducció de noms a adreces IP numèriques. El fet d'assignar un nom (p.e. www.upc.edu) a una adreça IP (p.e 147.83.20.2) permet als usuaris utilitzar noms en comptes d'haver de recordar un codi numèric. Un altre dels avantatges de DNS és que permet abstraure el nom de màquina de la seva adreça IP (poden així variar sense tenir que modificar el nom de la màquina).

El nom de qualsevol equip dins del sistema DNS pot arribar a tenir fins a 3 parts diferents: a) Un nom de domini, b) Un o més subdominis i c) Nom de l'equip. Els subdominis no són obligatoris per assignar un nom a un equip però el domini i el nom de l'equip sí que són necessaris. La unió de domini + subdominis (si existeixen) + nom d'equip rep el nom de Fully Qualified Domain Name o FQDN. Un exemple de FQDN seria www.clot.fje.edu, a on fje.edu és el nom de domini, clot és el subdomini i www és el nom de l'equip.

El servei DNS és jeràrquic. Els nom tenen una jerarquia que es pot visualitzar en forma d'arbre, a on tenim a) El Root Level (identificat amb un punt “. “) , b) Els top level domain com per exemple com, net, org, edu,... c) Els second level domain, com per exemple “fje” dins de www.clot.fje.edu, d) Els subdominis, com per exemple “clot” dins de www.clot.fje.edu, i els nom de l'equip (hosts) com per exemple “www” dins de www.clot.fje.edu.

El servei DNS és distribuït. Múltiples servidors de noms es reparteixen la càrrega de proveir de resol·lució de noms als clients, encarregant-se cadascú de diferents zones, dominis i subdominis de la xarxa. Aquesta manera de treballar normalment s'aplica quan es treballa amb sistemes jeràrquics.

DNS està format per una xarxa de servidors que de manera col·lectiva permeten accedir a una base de dades global, jeràrquica i distribuïda a on es pot trobar el nom de qualsevol equip i l'adreça IP que tingui assignada.

## **B) Alguna terminologia útil**

a) **Nameserver**: Servidor de noms DNS

b) **Resolver**: Client DNS. Programa cridat perquè s'encarregui de realitzar la consulta al servidor de nom DNS.

c) **Domini**: Conjunt dels equips (realm) que comparteixen el mateix nom de domini de segon nivell.

d) **Subdomini**: Conjunt dels equips que comparteixen el mateix nom de domini de segon nivell i el mateix nom de subdomini. Poden existir subdominis dins d'un subdomini.

e) **Zona**: Conjunt que pot estar format per:

\* Un o més dominis

\* Un o més subdominis

\* Un subconjunt d'equips i subdominis dins d'un domini

\* Un subconjunt d'equips i subdominis dins d'un subdomini.

El servidors DNS com per exemple **bind** de Linux treballen definint zones, tot i que moltes vegades una zona és igual a un domini. El conjunt d'equips que formen un domini pot estar dividit en diverses zones controlades per diferents servidors DNS.

f) **Query:** Petició que fa un client a un servidor per aconseguir l'adreça IP a partir d'un nom (o també es pot fer en sentit contrari).

g) **Autoritatiu o Autoritzat:** Servidor DNS que dóna una resposta a partir de dades aconseguides per ell mateix a partir dels seus fitxers locals, amb independència de com s'hagin aconseguit aquests fitxers. Un mateix servidor DNS pot ser autoritatiu d'una o més zones.

h) **Delegació de domini:** Es produeix per exemple quan un servidor DNS autoritatiu d'un domini rep una petició i en comptes de donar la resposta final, envia al client que realitza la petició l'adreça d'un altre servidor al qual ha delegat per ser l'autoritatiu d'aquell subdomini. Per exemple, si demano l'adreça IP de www.clot.fje.edu, el servidor DNS autoritatiu de fje.edu pot respondre amb l'adreça IP d'un servidor DNS que sigui autoritatiu sobre clot.fje.edu al qual ha delegat aquesta responsabilitat. Un altre exemple és quan els servidors DNS del domini de primer nivell .edu deleguen la seva resposta en el servidor DNS autoritari de fje.edu.

### **C) DNS master i slave**

1- **Servidor DNS primary master:** Obté la informació sobre una zona des d'un fitxer que es troba dins del propi ordinador.

2- **Servidor DNS secondary master:** Obté tota la informació sobre una zona des d'un altre servidor, que ha de ser autoritatiu de la zona i que és el seu servidor master. Aquesta informació es pot emmagatzemar en un fitxer.

3- El servidor master d'un servidor DNS secondary master és gairebé sempre el servidor primary master de la zona però no és obligatori perquè un secondary master podria aconseguir la seva informació des d'un altre secondary master.

4- Avui dia s'utilitza de manera preferent el nom slave per referir-se a un secondary master i el seu servidor DNS primary master s'anomena simplement "servidor DNS master".

5- El principal objectiu d'un servidor DNS slave és oferir redundància per protegir contra caigudes del servidor primay master, repartir la carrega, i assegurar-se de tenir sempre un servidor lo més a prop possible dels clients.

6- Quan un servidor DNS secondary master es posa en marxa, es connecta amb el seu servidor master i, si és necessari, recull la informació sobre la zona que es troba al seu servidor master. Aquest procés rep el nom de transferència de zona.

7- Tant un servidor primary master com un slave són servidor autoritatius d'una zona perquè si responen a una petició, ho fan a partir de la informació que tenen dins d'un fitxer que es troba al propi ordinador. La diferència és el mecanisme pel qual obté la informació de la zona.

8- Un servidor DNS pot ésser master per una o més zones i al mateix temps ser slave per altres zones.

9- Moltes vegades es diu que un servidor DNS és master simplement perquè és master

de més zones que slave d'unes altres, o sigui si un servidor DNS és master de 7 zones i slave de 3 llavors en general es diu que és un servidor DNS master. En canvi si és master de 3 zones i slave de 7 llavors en general es diu que és un servidor DNS slave.

#### **D) Servidor DNS cache**

1- Obté informació des d'un altre servidor DNS (un servidor DNS master de la zona) en resposta a una petició d'un client, envia aquesta informació al client, i després emmagatzema aquesta informació localment, o sigui, emmagatzema la informació a la caché (que està a la RAM o a la swap). A la següent petició realitzada, el servidor DNS caché respon amb la informació emmagatzemada a la seva caché.

2- La informació en la caché és vàlida fins que el valor TTL expira, i llavors haurà de refrescar les seves dades de la zona connectant-se amb el servidor master.

3- Si el servidor DNS respon a una petició connectant-se amb el servidor DNS master, llavors retorna una resposta autoritativa. Si respon amb la informació de la seva caché, llavors la resposta és no autoritativa.

4- Per defecte un servidor DNS cache només emmagatzema les respostes amb èxit a una petició DNS.

#### **E) Negative Caching**

1- Consisteix en emmagatzemar a la cache del servidor DNS el resultat de peticions sense èxit. Si per exemple, ens equivoquem i pensem que la web de l'escola és [www.elclot.fje.edu](http://www.elclot.fje.edu) i enviem una petició, el resultat serà que no existeix. Amb el Negative Caching aquest resultat s'emmagatzema per poder respondre ràpidament a futures equivocacions i que el servidor DNS no intenti fer el procés de resolució.

2- El període de temps que un servidor DNS manté un resultat negatiu queda enregistrat en el camp Minimum del SOA.

#### **F) REVERSE**

1- És difícil i lent fer recerca d'una IP i trobar nom perquè DNS està pensat per treballar amb noms i trobar IP (S'indexa pel nom).

2- Solució: Utilitzar IP com si fosin noms i crear un nou espai de noms. Aquest nou espai s'anomena in-address.arpa. O sigui, s'aprofita l'eina de busqueda directa per convertir-la en una eina de busqueda inversa també.

3- Domini invers:

arpa --> top level domain

in-addr.arpa--> nom del domini

0-255.in-addr.arpa -> subdomini de in-addr.arpa

0-255.0-255.in-addr.arpa --> subdomini de 0-255.in-addr.arpa

0-255.0-255.0-255.in-addr.arpa --> subdomini de 0-255.0-255.in-addr.arpa

0-255.0-255.0-255.0-255.in-addr.arpa --> subdomini de 0-255.0-255.0-255.in-addr.arpa

4- Quan busco un ordinador per IP, per exemple 192.168.1.10, es fa la recerca dins de l'arbre in-addr.arpa com si estigués buscant un ordinador de nom 10.1.168.192.in-addr.arpa. Un cop es troba el registre s'agafa el nom associat de la mateixa manera que s'hagués fet si és busqués de la manera habitual.

## **G) REGISTRE SOA**

1- Paràmetres globals de la zona :

a) **Nom del domini:** Es pot escriure, posar una directiva ORIGIN abans o @ => Es troba a partir del nom de la zona al fitxer named.conf.local

b) **Classe IN:** Tipus internet

c) **Servidor DNS:** Nom d'un servidor DNS que respondrà autoritativament. S'ha d'escriure el nom complet .

d) **Adreça correu electrònic** de l'administrador de la zona (sense arroba, perquè "." és el separador) .

e) **Número sèrie.**

f) **Refresh:** Cada quan un slave ha de refrescar les seves dades de la zona a partir del master. En segons. 32 bits.

g) **Retry:** Temps entre intents de refresh quan el slave falla amb contactar amb el master i el refresh ha expirat. En segons. 32 bits

h) **Expiry:** Un servidor DNS slave deixa de respondre de manera autoritativa a peticions DNS si ha passat aquest temps i no ha pogut contactar amb el master. 32 bits. Segons .

i) **Minimum:** Temps d'emmagatzematge d'un Negative Caching. (Valor màxim: 3h) .

## **I) ALTRES REGISTRES**

1- Adress IP Record --> **A:** A partir d'un nom es troba la seva adreça IP. S'utilitzen en els fitxers de zona que fan el mapat directe de nom a adreça IP.

2- Name Server Record --> **NS:** Dins d'un arxiu de zona, són registres autoritatius a on desa la informació sobre quins són els ordinadors que fan de servidors de noms de la zona.

3- Pointer Record --> **PTR:** A partir d'una IP es troba el nom de l'equip. S'utilitzen en els fitxers de zona que fan el mapat invers d'adreça IP a nom.

4- Canonical Name Record --> **CNAME:** Registres per escriure els alies d'un nom d'ordinador.

5- Mail Exchange Record --> **MX:** Especifica el nom i la preferència del servidors de correu de la zona.

## **H) DIRECTIVES \$TTL i \$ORIGIN**

1- La directiva **\$TTL**, dins del context del sistema DNS, defineix la durada en segons que el registre pot ser mantingut en caché.

2- La directiva **\$ORIGIN** defineix un nom base a partir del qual es completen el noms incomplets. Un nom és incomplet si no finalitza amb un punt (o sigui `.`). Bàsicament serveix per posar el nom del domini i subdomini darrera quan només s'escriu el nom del host en la configuració.