Protocol DNS

Conceptes bàsics

Els documents oficials on s'estableix el protocol DNS són els RFC (Request-For-Comments) següents: 1033, 1034, 1035, 1032 (que explica com registrar noms), 1918, 1912, 1713, 1712 i 2052. Es poden consultar a http://www.rfc-editor.org . Allà es defineixen els següents conceptes, entre d'altres:

FQDN (Fully Qualified Domain Name)	És el nom complet d´una màquina, incloent-t'hi tota la cua de dominis a la què pertany (té la forma, per tant, següent: *hostname.subdomini1.subdomini2.domini.tld*). L'anomenat "domini d'últim nivell" (o "TLD", de "Top Level Domain" és el que s'escriu a la dreta del punt de més a la dreta del FQDN (veure més endavant)
Zone	Bàsicament és un arxiu de text incloent una llista de parelles <nom>/<adreça IP>. Pot contenir la informació sobre un domini complet (i possiblement, els seus subdominis, si és que no es deleguen aquests en altres servidors), o sobre més d'un (rafa.com, dani.org ...) o sobre part d'un.
Resolver	És la part client del servei DNS. La seva funció és la de realitzar les peticions sol·licitant l'adreça IP d'un nom. Pràcticament totes les aplicacions de xarxa (des d'un ping fins a un gestor de correu, etc, etc) inclouen una llibreria/component que realitza aquesta funció.
Nameserver	És la part servidora DNS. La seva funció és la de contestar a les peticions de noms rebudes. Escolta normalment al port 53 UDP. Només en determinats casos (en una transferència de zona, o bé quan la petició supera els 512 bytes -estrany-), s'utilitzarà el port 53 Tcp.
Authoritative nameserver	Servidor responsable d'una zona (és a dir, el que conté físicament els arxius de zona, i on l'administrador dels modificarà si és el cas). Per a cadascuna de les zones que puguin existir ha d'haver sempre com a mínim un servidor que s'encarregui de la seva gestió. Les respostes relacionades amb la seva zona que donarà als clients es diuen respostes "autoritatives", perquè són respostes "de primera mà"
Recursive nameserver	Si un nameserver rep una petició de resolució i no coneix la resposta perquè no posseeix l'arxiu de zona amb la informació demanada, realitza al seu torn totes les peticions que siguin necessàries a altres servidors DNS per accedir a la zona corresponent que contingui la resposta, de manera que li pugui donar a el client la informació encara que no disposi d'ella en un primer moment. NOTA: Aquesta capacitat recursiva és configurable, de manera que no sempre els servidors realitzaran tot aquest procés de recerca completa. Si no ho fa, el servidor en qüestió al menys haurà d'indicar al client a quin altre servidor pot preguntar (és a dir, "es renta les mans", en el que es coneix com a "mecanisme de delegació"); d'aquesta manera tot el treball va a càrrec del client, ja que aquest haurà de tornar a preguntar al nou servidor indicat. Aquest tipus de consultes no recursives es diuen consultes iteratives, tot i que no són molt habituals.
Cache nameserver	Servidor DNS que no defineix cap zona: només conté la memòria cau de consultes anteriors a altres servidors DNS, realitzades (gairebé) sempre de forma recursiva. Per tant, les seves respostes mai seran autoritatives. Però llavors, ¿per què interessa tenir només un servidor DNS de memòria cau en una xarxa local? Perquè s'agiliti l'accés a Internet: gràcies a que la majoria de respostes ja estaran dins de la memòria cau de servidor local, no s'haurà de sortir a fora per a cada petició Dns que es realitzi; la durada de la informació en la memòria cau de servidor ve definida per un camp de la seva configuració anomenat TTL (Time To Live). D'altra banda, tot client ("resolver") DNS també disposa de la possibilitat de consultar una memòria cau local per tal de ni tan sols haver d'anar així a preguntar a cap servidor DNS si la informació ja ha estat prèviament obtinguda. A Windows aquesta memòria cau local es pot consultar (i esborrar, respectivament) amb: *ipconfig /displaydns* i *ipconfig /flushdns*; a Linux l'esborrat es pot realitzar amb la comanda *resolvectl flush-caches* i la consulta encara no es pot fer (veure https://github.com/systemd/systemd/issues/14796)
Forwarding nameserver	Servidor DNS que passa totes les peticions a un altre servidor DNS remot (sovint de tipus cau). La gràcia està en que aquests servidors guarden les respostes (és a dir, funcionen també com a servidors cau) però no fan consultes recursives sinó que "passen el marró" al servidor DNS remot.

Root server	El sistema de DNS proporciona un conjunt bàsic de servidors arrel (també anomenats ".") de manera que a partir d'ells es pugui resoldre qualsevol petició. Aquesta llista de servidors bàsics és "fixa" (consta de 14 servidors per tot el món, nomenats mitjançant lletres de l'abecedari), i està permanentment emmagatzemada en tots els programaris servidors DNS existents (Bind, dnsmasq, etc.). Es pot consultar la seva existència en http://www.root-servers.org i teniu més informació a https://www.iana.org/domains/root/files
gTLD & ccTLD nameserver	Un "Top Level Domain server" és el servidor que conté tota la informació referent a un domini d'últim nivell, els quals poden ser de dos tipus: geogràfics ("Country Code TLD") o genèrics ("Global TLD"). Un exemple dels primers seria el ".es" i un dels segons, el ".com". Hi ha un nombre limitat de TLDs, generalment mantinguts per governs o entitats reconegudes sense ànim de lucre (respectivament). La llista es pot consultar aquí: http://www.iana.org/domains/root/db
Zone transfer	Transferència de la informació que conté un servidor **mestre (primari)** en els seus fitxers de zona, a un altre anomenat **esclau (secundari)**. El servidor mestre és el que manté la zona (llegeix la informació de l'arxiu i pot fer modificacions en ella), i el servidor secundari simplement agafa les dades periòdicament del primari i les manté en la seva memòria RAM. El servidor secundari no pot fer modificacions en la zona, però té la mateixa autoritat que el mestre: l'única diferència és que en el servidor mestre els arxius de zona estan guardats físicament i es poden editar manualment mentre que a l'esclau no existeixen els fitxers físics perquè la seva informació ha estat descarregada directament a la seva memòria RAM. El motiu de l'existència dels servidors esclaus és la disponibilitat del servei DNS: si en algun moment un dels dos servidors cau, l'altre pot seguir treballant sense que el servei se'n ressenti. De fet, el RFC 2182 requereix que hi hagi al menys dos servidors DNS per cada zona. No confondre servidor secundari amb servidor de memòria cau: no tenen res a veure. El primer té tanta autoritat com el primari (només que les seves zones les obté d'aquest), i el segon solament pot respondre per la informació que anteriorment va obtenir d'altres peticions a servidors autoritatius.
Resource record	A més de la traducció <nom>/<adreça IP> que ja hem comentat, els nameservers també poden proporcionar altres tipus d'informació útil. Exemples d'això poden ser l'obtenció dels possibles "àlies" d'un nom (registres **CNAME**), l'obtenció de l'associació d'un nom amb IPs de versió 6 (registres **AAAA**), l'obtenció dels servidors DNS autoritatius del domini en qüestió (registres **NS**), l'obtenció dels servidors de correu pertanyents al domini en qüestió (registres **MX**), etc

NOTA: Per una explicació més detallada podeu consultar els articles https://www.digitalocean.com/community/tutorials/a-comparison-of-dns-server-types-how-to-choose-the-right-dns-configuration i https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts

Procés d´una petició de resolució de noms

Per exemplificar el funcionament del DNS realitzarem una petició de "ping" a www.rediris.es, per exemple.

1.-El primer que farà el nostre ordinador és enviar una petició al nostre servidor de noms preferit sol·licitant-li la direcció IP de www.rediris.es. Òbviament per al nostre exemple hem d'assumir que cap petició es troba a la memòria cau (lloc on es guarden les peticions ja realitzades) dels servidors. Això ens permetrà analitzar en detall tot el procés.

2.-Un cop sol·licitada la petició al nostre servidor de noms, aquest comprova que no coneix la resposta i consulta llavors la seva base de dades interna de Root servers (totes les aplicacions servidores DNS la porten incorporada de sèrie) per triar un a l'atzar. Aquest mecanisme de selecció aleatori té com a objectiu evitar el col·lapse d'un únic servidor balancejant les peticions entre els diferents elements del conjunt. Un cop seleccionat un dels servidors genera una petició per reenviar la consulta sobre el nom de www.rediris.es. El Root server que rep la petició comprova que no coneix la resposta i llavors respon proporcionant un servidor gTLD que gestiona el domini sol·licitat (".es" en el nostre cas).

Simplificant-ho molt, imagina que la "zona" que controla un Root Server és simplement una llista de IPs dels diferents servidors DNS gTLD que coneix, als quals preguntarà en rebre una petició que correspongui amb la seva gTLD corresponent; així per exemple, podríem tenir el següent:

.com	14.164.201.78
	32.56.143.234
	89.67.122.236
.org	67.45.111.132
	154.213.213.2
.net	56.34.213.143

3.-Una vegada rebuda la IP d'un servidor autoritatiu gTLD del domini ".es" el nostre "recursive nameserver" li envia una nova petició de sol·licitud de resolució de nom per www.rediris.es. El servidor gTLD comprova que no disposa de la resposta i llavors busca a la base de dades quins servidors s'encarreguen del domini de segon nivell de la petició (rediris.es en el nostre cas).

Simplificant-ho molt, imagina que la "zona" que controla un servidor gTLD és simplement una llista de IPs dels diferents servidors DNS de segon nivell per a aquest gTLD, als quals preguntarà en rebre una petició que correspongui amb aquest domini corresponent; així, per exemple, per a un servidor gTLD .edu podríem tenir el següent:

pepito.edu	14.164.201.78
	32.56.143.234
	89.67.122.236
manolito.edu	67.45.111.132
	154.213.213.2
jaimito.edu	56.34.213.143

4.-Un cop més el nostre "recursive nameserver" rep una contestació negativa a la seva pregunta juntament amb un nou servidor on ha d'anar a preguntar. Així doncs torna a fer la petició de resolució de nom per www.rediris.es i l'envia al servidor encarregat de gestionar el domini "rediris.es". Finalment rep una contestació afirmativa on s'explicita que l'adreça IP associada a la màquina amb nom www.rediris.es és 130.206.1.22.

Simplificant-ho molt, imagina que la "zona" que controla el servidor cocacola.com és simplement una llista de IPs de les diferents màquines que formen aquest domini com la mostrada a continuació. D'aquesta manera, quan rebi una consulta preguntant sobre una màquina concreta del seu domini, respondrà retornant la IP associada:

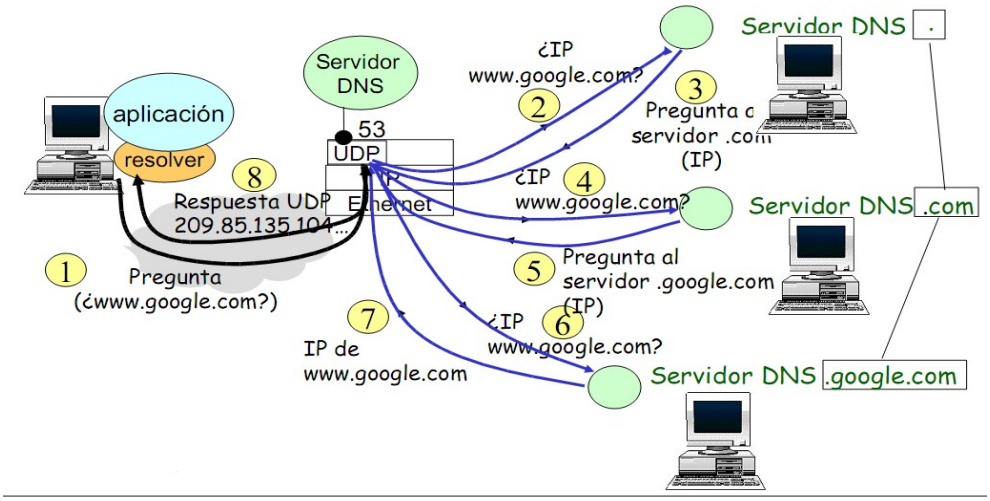
www.cocacola.com	14.164.201.78
smtp.cocacola.com	67.45.111.132
unpc.cocacola.com	154.213.213.2
otropc.cocacola.com	56.34.213.143

5.-Un cop resolta la petició original pel "recursive nameserver", aquest envia la resposta a l'usuari inicial, que realitzarà al seu torn una connexió a l'adreça IP proporcionada.

6.-Cal destacar que el sistema de memòria cau de DNS s'encarrega d'emmagatzemar les últimes peticions que es realitzen pels usuaris de manera que no sigui necessari realitzar aquest procés incomptables vegades cada segon per a cada usuari. Però per altra banda, el sistema de DNS marca cadascuna d'aquestes respostes amb un període de validesa finit de manera que els nous canvis que es poguessin realitzar en alguna zona puguin ser "visibles" al cap d'un període de temps concret.

NOTA: En el cas de l'enviament de correu electrònic, el procés és similar: una vegada que el correu a emetre ha arribat al servidor SMTP predefinit en el client, per lliurar-lo al destinatari aquest servidor SMTP sol·licita al servidor DNS que tingui configurat el valor del registre MX del domini del receptor del missatge; quan el rep, es connectarà al seu port 25 i el lliurarà (cal dir que el procés pot continuar si el receptor del missatge no és l'últim de la cadena, ja que hi ha servidors que actuen com gateways entre dominis).

A continuació es mostra un diagrama on es mostra gràficament el procés descrit als paràgrafs anteriors:



Informació que pot haver emmagatzemada en una zona

Als arxius de zona no només hi ha informació sobre què nom correspon a cada IP, hi ha més informació. Per identificar el tipus d'informació, s'especifica el seu “tipus” amb un codi clau (“A”, “MX”, etc), que indica quina informació és la que hi ha emmagatzemada en concret. A continuació es llisten els "tipus" d'informació (tècnicament anomenats "registres") que solen emmagatzemar més habitualment el servidors DNS:

Registre **A**	Tradueix noms de hosts del domini a IPs. És la informació “per antonomàsia” que esperem trobar en qualsevol arxiu de zona.
Registre **AAAA**	El mateix que l´anterior però per IPv6
Registre **CNAME**	Indica un àlies per un host determinat (definit por A)
Registre **MX**	Indica el servidor SMTP encarregat de rebre el correu electrònic per aquell domini
Registre **NS**	Indica el/s servidor/s de noms autoritatius d'un domini (els servidors primaris i secundaris que mantenen la zona). Permet així que els diferents servidors DNS es reconeguin entre si quan es realitzin consultes recursives entre ells, ja que el que miraran serà el valor d'aquest registre per saber a qui han de preguntar. Aquest registre també permet la delegació de dominis, ja que si es produeix, existirà (a més dels servidors primari i secundaris ja comentats deel domini superior) un registre NS per cada responsable de cada subdomini delegat.
Registre **HINFO**	Afegeix informació textual addicional relativa a un host de domini, com la seva CPU, SS.OO, etc
Registre **TXT**	Afegeix informació textual addicional. Es pot fer servir, per exemple, per emmagatzemar claus de xifrat, o per filtrar spam mitjançant servidors de llistes negres DNSBL, o per utilitzar VPNs, etc.
Registre **PTR**	Tradueix IPs a noms de hosts del domini (registre invers)
Registre **SOA**	Indica vàries dades administratives importants, com ara la direcció de correu de l´administrador, el número de sèrie del domini, paràmetres d´actualització de la zona,etc). La seva existència per si sola ja indica que el servidor que conté l´arxiu de zona on apareix és un servidor autoritatiu.
Registre **SRV**	Informa de serveis específics disponibles a través del domini. Ho fan servir protocols com SIP o XMPP per a què els clients descobreixin de forma automàtica els serveis disponibles al domini.
Registre **ANY**	Tots els registres (utilitzat per dig)

Veure https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml per conèixer la llista completa de RRs

Estructura d'un paquet DNS (de petició i de resposta)

Dins del "payload" d'un paquet DNS podem trobar els següents camps, entre d'altres (per obtenir la llista completa, consulteu http://www.newdevices.com/tutoriales/dns/3.html o inspeccioneu tràfic DNS amb Wireshark):

*Camp ID: És un identificador de 16 bits que el sistema operatiu utilitza per distingir entre consultes. D'aquesta manera es pot saber a quina consulta correspon cada resposta que arriba (l'ID de resposta és el mateix que el de la consulta). No caldrà especificar-lo a mà perquè el sistema operatiu ja li assigna un valor adient automàticament

*Camp FLAGS: Conté diferents valors independents, entre els quals podem destacar:

*QR: Tipus de missatge (0 = consulta , 1 = resposta). Si no s'indica, per defecte és 0
*OPCODE: Tipus de consulta (0 = estàndar , 1 = inversa, 2 = petició d'estat de servidor). Si no s'indica, per defecte és 0
*RD: Indica si es vol una resposta recursiva (1) o no (0). Si no s'indica, per defecte és 0

*Camp de petició (QD) : Està format al seu torn bàsicament per dos camps:

*QNAME : Nom de domini/host (ha de començar amb \n i el punt s'ha d'escriure amb 0x03)
*QTYPE : Registre a consultar ("A" -1 en hexadecimal-,"CNAME","AAAA","NS",…)

*Camp de resposta (RD) : Present només a les respostes, conté la informació requerida.