Exercici 11 - DNS i DHCP

PART 1 - Conceptes sobre DNS

1- Què és un nom **FQDN** (Full Qualified Domain Name) d'un equip?.
És el nom pel qual identifica de manera completa un equip i està format per una llista de noms separats per punts. Per exemple, un nom FQDN seria:

www.fje.edu.

Normalment, el darrer punt no s'escriu i per tant la manera habitual d'escriure el nom FQDN de l'exemple seria:

www.fje.edu

2- Què és **DNS**?
DNS és un servei que mapejar noms d'ordinadors a les seve adreces IP i viceversa. Per fer aquest feina el servei DNS:

- Està organitzat d 'una manera jerarquica i distribuida
- Utiliza noms de domini

3- Què és un **domini** del servei DNS?. Què és un **nom de domini**?.
És un conjunt d'equips informàtics els noms dels qual s'administren i s'assignen d'una manera independent als d'altres equips que formin part d'un domini diferent.

Un domini s'identifica pel seu nom de domini. Tots els equips d'un mateix domini comparteixien, dins del seu FQDN, un mateix nom de domini. Per exemple, mail.fje.edu i www.fje.edu formen part del mateix domini fje.edu.

4- Què és la Jerarquia DNS?
Els noms de domini estan organitzats per ordre d'importància en els següents nivells:

- Domini arrel (que no té nom) i s'identifica amb un **.** i normalment no s'escriu explicitament
- El Top Level domains → .org .edu .com .es .uk .info
- El Sencondary Level domains → fje google facebook binefa etc. Aquests es poden registrar, és a dir, una empresa o persona pot tenir el seu propi secondary level domain.
- Tertiary domain level → Normalment els anomenem subdominis
- Nom base d'un equip informàtic.

5- Què vol dir que el servei DNS està distribuït?
Que l'autoritat sobre cada domini i els seus noms i IPs no recau sobre una autoritat central sino que es reparteix entre tots els administradors i servidors DNS que controlen cada nivell i cada nom de domini.

Evidentment, a cada nivell es confia que els servidors i administradors dels nivells superiors i inferiors fan bé la seva feina.

Per exemple, l'administrador i el servidor DNS que controla el domini **fje** dins del domini **edu**, o sigui **fje.edu** confia en que:

- En que els administradors i servidors DNS de **.edu** fan la seva feina
- En que els administradors i servidors DNS de **clot.fje.edu** fan la seva feina

6- Què és la **caché DNS**?.
Un espai de memòria a on podem emmagatzemar consultes DNS prèvies. Permet recuperar un registre DNS que ja hem consultat sense haver d'enviar la petició al servidor DNS. Això permet trobar la informació de manera més ràpida.

7- Què és un servidor **DNS autoritatiu**?. Que és un DNS servidor **no autoritatiu**?.Què és un servidor **DNS caché**?. Pot ser un servidor DNS autoritatiu i caché al mateix temps?.

Aquell que quan respon a la petició feta per un client que demana saber l'adreça IP a partir d'un nom, respon amb autoritat perquè és el servidor que és la font original de la informació demanada. Altres servidors recuperen aquesta informació de la cache però aquest servidor té la informació original que utilitzen els altres servidor i a més a mé, és informació actualitzada, confiable i registrada per l'administrador del servei.

Un servidor DNS no autoritatiu no és la font original de les dades, la seva informació potser està desactualitzada, no és confiable i no va ser registrada per l'administrador del servei.

Un servidor DNS caché respon a la petició feta per un client que demana saber l'adreça IP a partir d'un nom amb la informació que té a la seva cache DNS, i per tant, no és la font original de les dades, la seva informació potser està desactualitzada, no és confiable i no va ser registrada per l'administrador del servei. Per tant, no és un servidor autoritatiu.

Sí, un servidor DNS pot ser autoritatiu per un domini i caché per un altre domini.

8- Què és una **resposta autoritativa** i una **resposta no autoritativa**?

Autoritativa → Quan la resposta a una petició la dóna el servidor DNS autoritatiu.
No autoritativa → Que la resposta a una petició la dóna un servidor no autoritatiu.

9- Quina informació poden donar de manera **autoritativa** els servidor **DNS autoritatius** de:

- el **root domain**: Del servidors DNS autoritatius del dominis TLD (org, edu,...)
- els **top level domains**: Del servidors DNS autoritatius del dominis de segon nivell (fje.edu, google.com, binefa.net,.....)
- els **secondary levels domains**: Poden informació de manera autoritativa sobre IPs i noms d'equips o de servidors DNS autoritatis de subdominis.
- els **subdomini**s o **tertiary levels domains**: Poden informació de manera autoritativa
- sobre IPs i noms d'equips i de DNS de subdominis de nivell inferior.

10- En què consisteix el sistema **DNS recursiu**?

Que si consultem a un servidor DNS d'un nivell superior i no té la informació demanada en la caché envia a l'ordinador client la IP del servidor DNS autoritatiu de nivell inferior que pot donar-li la resposta.

11- Quines són les parts de les quals **es composa un FQDN** d'un equip?.

En general serien aquestes les parts:

fqdn=nom base + tertiary level domain (opcional) + secondary level domain + top level domain + root domain

Per exemple:

www.clot.fje.edu. = www + clot + fje + edu + .

A on:

- www = nom base
- clot = tertiary level domain
- fje = secondary level domain
- edu = top level domain
- . = root domain

Cal recordar que el root domain normalment no s'escriu explicitament.

12- Què és el **nom base** d'un equip?. A què identifiquem, tot i que no sigui totalment correcte, com el domini d'un equip?.

El nom base o nom de host d'un equip és la part del FQDN que hi ha abans del nom de domini de segon nivell. Només accepta els caràcters 'a-z', 'A-Z', '0-9', i '-'. Tot i que sigui una pràctica habitual, el nom de l'equip no és obligatori que tingui relació amb els serveis que dóna.

El domini normalment es considera que és la suma del nom de domini de segon nivell + el top level domain. Per exemple collados.org es considera el domini d'un equip tot i que realment, és la combinació del seu nom de domini de segon nivell collados i del TLD .org.

12- Què és un **registre de recurs**?. Què és una **zona DNS**?
Un servidor DNS emmagatzema dins del registres de recursos la informació necessària per donar el sevei de resolució de noms. Per exemple, aquests registres de recursos emmagatzemen la informació per poder associar el nom d'un equip a la seva adreça IP.

Aquests registres s'emmagatzemen dins del caché DNS o dins dels fitxers de zona DNS. Un registre serà una entrada dins del fitxer de zona DNS.

Una zona DNS és un espai de noms DNS gestionats per un mateix servidor DNS autoritatiu de la zona. En el cas més simple, una zona serveix per definir tot l'espai d'adreces d'un domini DNS.

13- Quin són alguns dels **registres de recursos** més important?

Alguns dels registres DNS més importants són:

- Registres tipus A i AAAA → El registre A serveix per proporcionar l'adreça IPv4 d'un equip a partir del seu FQDN d'ordinador. El registre AAAA serveix per proporcionar l'adreça IPv6.
- Registre NS → Serveix per proporcionar el nom del servidor DNS autoritatiu del domini.
- MX → Serveix per proporcionar els noms dels servidor de correu del domini. Tenen un número per indicar la prioritat dels servidors.
- PTR → A partir d'una adreça IPv4 o IPv6 proporciona el FQDN d'un equip.
- SOA → Dóna informació general com per exemple, dades sobre l'administrador, sobre caché de DNS, etc..
- CNAME → Alias d'un nom d'equip. Per exemple mail.collados.org pot ser un nom alias (o alternatiu) de server.collados.org.

14- A on es troben els **registres de recursos** dins d'un servidor **DNS autoritatiu**?
Els registres de recursos s'emmagatzemen en el cas de Linux dins dels fitxers de zona DNS, que són fitxers de text que es troben normalment a /var/cache/bind. En el cas de Windows, el registres de recursos i les zones estan integrades dins de l'Active Directory.

15- Què és el **protocol DNS**? De quin **nivell** del model **TCP/IP** és?
Explica els passos a seguir per un client DNS fer una petició al servidor DNS i de els passos a seguir per enviar la resposta des del servidor DNS. Per fer això cal que servidor i client s'enviïn entre ells missatges DNS. El protocol també explica com és un missatge DNS, o sigui, els camps que té i per a que serveixen.

16- Què és un **missatge DNS**?. S'encapsula dins d'un datagrama UDP o un segment TCP?
Són els missatges que s'envies els clients DNS i els servidors DNS per fer consultes en la base de dades DNS del servidor i rebre respostes el client. Els servidors i clients DNS són programari de nivell d'aplicació.

El servei DNS treballa conjuntament amb el protocol UDP. Ho podem veure obrint la captura DNS de la part pràctica 2.

17- Quin **número** i **tipus** de **port** utilitza un **servidor DNS**?. I un *client DNS*?
Mirant la captura de wireshark de la part 2 de la pràctica observem que el servidor DNS treballa amb el port 53/udp. El port UDP del client és dinàmic i generalment té un valor alt (generalment 30000 cap amunt).

18- Quins son **els 2 tipus de missatges DNS típics**?. Com els identifiquem?
Missatges de petició per part del client al servidor. En aquest cas el client normalment envia una pregunta al servidor. Aquesta pregunta normalment es demanar l'adreçaIP d'un equip.

Missatges de resposta del servidor al client. El servidor normalment envia una resposta al client indicant per exemple l'adreça IP d'un equip del qual el client només sabia el nom.

Si el primer bit del camp Flags val 0 llavors és una petició, però si en val 1, llavors és una resposta.

19- Com **identifiquem** i associem una **consulta** amb una **resposta**?
En un missatge DNS hi ha un camp que es diu Transaction ID. Quan es fa una petició el client introdueix un codi hexadecimal dins del Transaction ID per identificar la petició. És un valor de 2 bytes. El servidor quan respon utilitza aquest mateix valor per identificar la resposta i que el client a quina pregunta està associada.

20- Com sabem la **quantitat** de registres de recursos demanats pel client al servidor dins d'un missatge de petició?
En un missatge DNS de petició el camp Questions té un valor que indica al servidor quantes preguntes fa el client dins del missatge.

21- Com sabem concretament **quins registres de recursos** ha demanat el client al servidor dins d'un missatge de petició?
Per saber les preguntes concretes que ha fet el client al servidor hem de mirar el contingut del camp Queries del missatge enviat pel client.

22- Com sabem la **quantitat de registres de recursos enviats** pel servidor al client dins d'un missatge de resposta?
La quantitat de de registres de recursos enviats és igual al número de respostes lel servidor al client. Per saber la quantitat de respostes hem de mirar el camp Answer RRs d'un missatge enviat pel servidor. En aquest cas poden ser respostes autoritatives i no autoritatives.

23- Com sabem la **quantitat de respostes autoritatives** enviades pel servidor al client dins d'un missatge de resposta?
Per poder afinar una mica més, un missatge DNS de resposta té un camp de nom Authority RRs. Aquest camp indica el número de respostes DNS autoritatives enviades.

24- Com sabem concretament les **respostes enviades** pel servidor al client dins d'un missatge de resposta?
El camp d'una resposta DNS a on podem trobar les respostes enviades pel servidor es diu Answers.

25- Com sabem l'**adreça IP del servidor o servidor autoritatius d'un domini** dins de la resposta enviada per un servidor a un client?
Es troba dins del camp Authoritative nameservers.

PART 2 - Wireshark

1.- Descarrega el fitxer de wireshark http://www.collados.org/asix2/sm7/a1/wireshark/dns.pcapng. Posa en marxa wireshark i obre el fitxer **dns.pcapng**. Crea el **filtre dns**. Obre la primera captura. Expandeix el missatge *DNS*. Respons a les següens preguntes:

a) Quin és el tipus de missatge DNS: de petició resposta?.

És de petició.

b) Quin és el valor que identifica la petició?

El camps Flags val 0x0100. Això vol dir que el primer bit del camp Flags val 0 i per tant el missatge és de petició.

c) Quantes registres es demanen al servidor?

Per cada registre demant el client fa una pregunta al servidor, de manera que per respondre aquesta pregunta hem de mirar el valor del camp Questions que, en aquest cas, val 1. Per tant, el client fa només una pregunta al servidor.

d) De quin tipus és el registre demanat?.

Això ho sabrem mirant la pregunta que fa el client al servidor, que es troba dins del camp Queries. Si expandim Queries podem veure que demana un registre de tipus A, és a dir, una IPv4 a partir d'un nom.

e) Què es demana al servidor?

Està demanant l'adreça IPv4 de l'equip www.collados.org.

2.- Expandeix el missatge DNS de resposta a la petició de la pregunta 1. Respons a les següents preguntes:

a) Quin és el número de captura que has utilitzat?. Per què?

Hem buscat a captura de petició el valor dins del camp Transaction ID i hem vist que el valor era igual a 0x36f5 (36f5 en hexadecimal). Hem buscat una altra captura que tingués el mateix Transaction ID i hem vist que és la captura número 4. Ara haurem de comprovar que sigui de resposta.

b) Com saps que és de resposta?

El valor del camp Flags és 8180 en hexadecimal, i això vol dir que el primer bit val 1. Per tant és un missatge de resposta del servidor.

c) Quantes respostes ha enviat el servidor?

Per cada registre enviat el client dóna una resposta al servidor, de manera que per respondre aquesta pregunta hem de mirar el valor del camp Answer RRsQuestions que, en aquest cas, val 1. Per tant, el client fa només una pregunta al servidor.El valor de Answer RRs que en aquest cas val 2. Aixió doncs, el servidor ha enviat 2 respostes, tot i que el client només havia fet 1 pregunta.

d) Quantes respostes són autoritatives?

El valor Authority RRs és 0 i per tant, cap resposta és d'un servidor DNS autoritatiu.

e) Les respostes les ha trobades a la seva caché o a la seva base de dades?.

Estaven a la caché del servidor DNS

e) Què diu la primera resposta sobre www.collados.org.?

Si mirem el camp Answers, la primera resposta és un registre CNAME que en diu que www.collados.org. en realitat és un alies de collados.org (el nom canònic). És per aquest motiu que el servidor envia una segona resposta. La següent resposta ha de donar-nos el registre A de collados.org.

f) Què ens diu la segona resposta?

Ens envia el registre A de collados.org i per tant, ens diu que 156.67.24.117 és l'adreça IP de collados.org i, per tant, també de www.collados.org.

PART 3- nslookup

1- Troba amb nslookup:

- El nom i adreça IP de www.collados.org.
  156.67.24.117, que és el valor Address que correspon al valor Name de collados.org
- Indica si la resposta s'ha obtingut del servidor DNS autoritatiu de collados.org.
  Gairebé segur que és No Autoritativa perquè probablament la resposta la dóna el servidor DNS local de la teva xarxa o el servidor DNS del teu proveïdor d'accés a Internet.
- Indica l'adreça IP del servidor DNS que t'ha donat la resposta.
  Aquest valor depén del lloc i xarxa en el qual ens trobem. Per exemple, dins de l'escola, el servidor DNS serà el 172.20.254.100 perquè l'escola té el seu propi DNS server i aquesta és la seva adreça.

2- Troba amb **nslookup**:

- El veritable nom del servidor web **www.cisco.com.**
  El nom canònic (CNAME) de www.cisco.com és www.cisco.com.akadns.net
  El CNAME de www.cisco.com.akadns.net és wwwds.cisco.com.edgekey.net.globalredir.akadns.net
  El CNAME de wwwds.cisco.com.edgekey.net.globalredir.akadns.net és e2867.dsca.akamaiedge.net
  Així doncs, el nom real és: e2867.dsca.akamaiedge.net
- Les 2 adreces IPv6 del servidor trobat.
  2a02:26f0:980:59b::b33 (2a02:26f0:0980:059b:0000:0000:0000:0000:0b33)
  2a02:26f0:980:5ab::b33 (2a02:26f0:0980:05ab:0000:0000:0000:0000:0b33)