Lab 7. Domain Name System (DNS)

1. Introducció

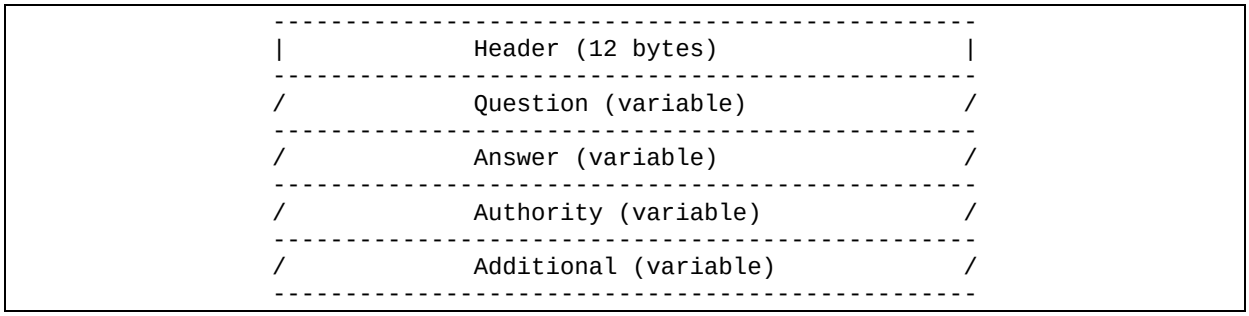
En aquesta pràctica s'aprofundirà en els protocol DNS. Per dur a terme els experiments que es detallen en l'enunciat utilitzarem una de les màquines del laboratori com a servidor DNS.

2. DNS

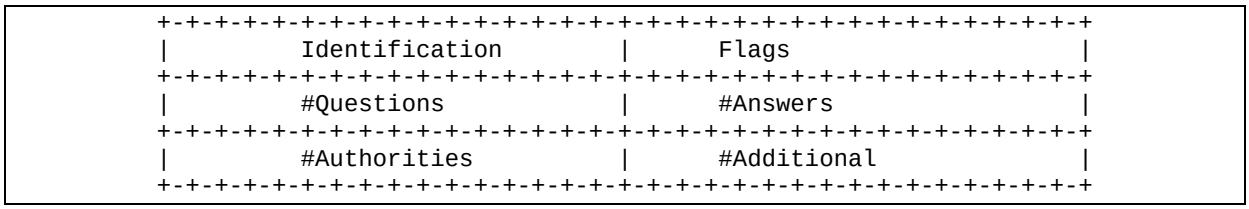
Aplicació client-servidor que es fa servir per la resolució de noms (conversió d'un nom en una adreça IP entre d'altres). Consisteix en una base de dades distribuïda. Les entrades s'anomenen Resource Records (RR) i poden ser de tipus:

- SOA: Start Of Authority.
- NS: NS name.
- MX: the domain mail exchange.
- A: A host address.
- CNAME: Canonical Name Record. E.g. the real hostname of www.foo.org is server.foo.org.

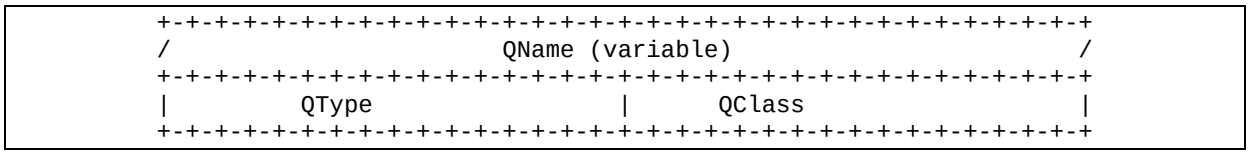
Tots els missatges DNS tenen el format:



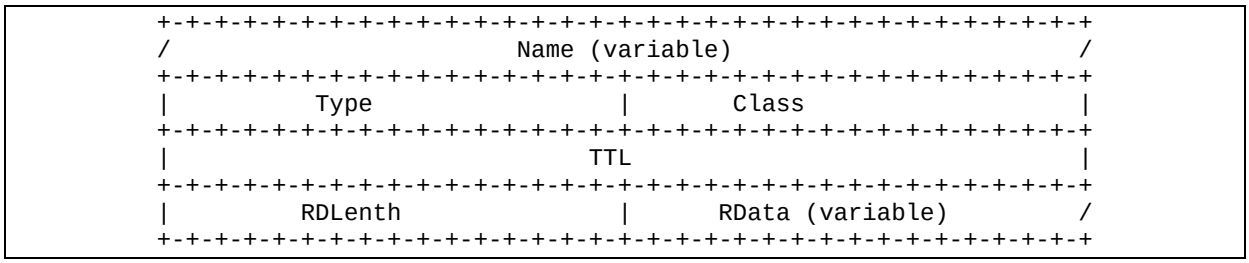
On la capçalera (header) és:



El camp question:



I els camps Answer, Authority i Additional són RRs:



3. Comandes bàsiques

Per a la realització de la pràctica es faran servir les següent comandes:

3.1. Wireshark

Wireshark és una eina d'anàlisi de xarxes. Permet monitoritzar el tràfic que circula per una interfície de xarxa amb una interfície gràfica. És l'equivalent gràfic a la comanda tcpdump. En aquest laboratori utilitzarem aquesta eina

per a veure com circulen per la xarxa de l'aula els missatges de nivell aplicació que s'intercanviaran durant la realització de la pràctica.

Per a posar en marxa el wireshark cal que executeu com a usuari root la comanda 'wireshark' (teniu una icona disponible a la barra de tasques de l'escriptori). Es necessari ser root perquè l'eina monitoritza tota la informació que circula per la interfície de xarxa independentment del procés i/o usuari que generi les dades, de manera que permet espiar l'activitat de xarxa dels altres usuaris que treballin en l'equip on s'executa el wireshark.

Un cop el programa és en marxa, podem anar al menú 'capture->interfaces' (o directament fer click en la icona que hi ha més a l'esquerra), triarem la interfície (eX) que disposi d'adreça IP, i polsarem 'capture' per a inicial la captura de paquets (veure la Figura 35). Un cop hagi finalitzat l'activitat que volem capturar, caldrà prémer el botó 'stop'.

Figura 35: Captura amb wireshark.

Un cop feta la captura podem filtrar els missatges d'un protocol concret, com mostra la Figura 36. Una característica molt important és la capacitat de poder seleccionar els paquets que volem capturar. Això es fa amb el quadre de text que hi ha al costat de Filter. Aquí hi podem posar una expressió com ara "dns" per capturar missatges que porten informació de nivell d'aplicació relativa al protocol http, o expressions més sofisticades com ara udp.port==53, per a capturar els segments UDP que porten el port font o destinació igual a 53.

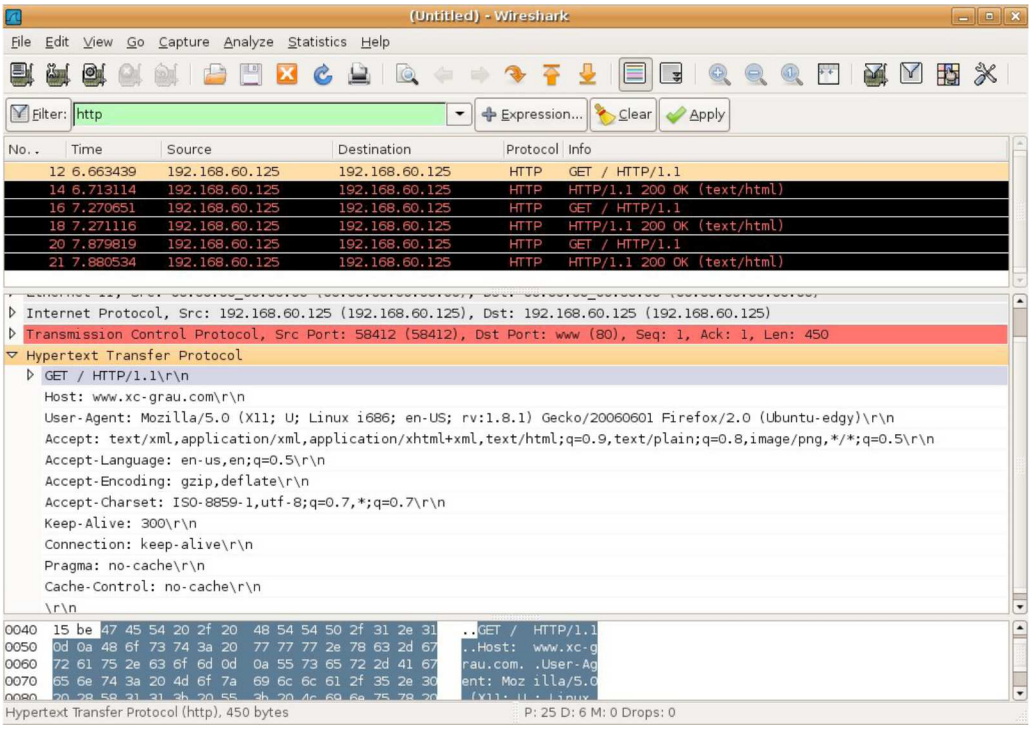


Figura 36: Filtre dels missatges http amb wireshark.

3.2. Comanda `dig`

Comanda per interactuar amb un servidor de noms (NS). S'invoca com:

```
dig [@server] [-p port#] [-t type] [-v] [-x addr] [name] [type] [opt...]
```

A continuació una explicació dels arguments:

server	El nom o l'adreça IP del servidor de noms a consultar. Si no es proporciona cap argument de servidor, dig consulta el servidor de noms a /etc/resolv.conf

name	El nom del registre del recurs que s'ha de cercar. Si un nom no té un punt final, la llista de cerca s'utilitza per qualificar (completar) el nom.
type	Cal el tipus de consulta: ANY, A, MX, PTR, SOA, NS, etc. pot ser qualsevol tipus de consulta vàlida.
opt	Diverses opcions:
+[no]recurse	Commutar la configuració del bit RD (recursió desitjada) a la consulta. Aquest bit està activat per defecte.
+[no]trace	Commutar el seguiment del camí de la delegació des dels servidors de noms arrel per al nom que s'està buscant.
+[no]short	Proporcionar una resposta concisa. El valor predeterminat és imprimir la resposta detallada.

Algunes preguntes útils:

Quina és l'adreça IP d' lloc web?
$ dig www.ac.upc.edu

Com s'identifiquen els servidors de noms associats amb un domini?
$ dig NS upc.edu +short
$ dig NS edu. +short

Quins servidors de correu electrònic són els responsables d'un domini?
$ dig MX ac.upc.edu +short

Quin és el nom de domini associat a l'adreça IP (cerca inversa d'IP)
$ dig -x 1.1.1.1 +short
$ dig -x 147.83.0.1 +short

Quin és el camí de delegació per a qualsevol zona DNS (com funciona el DNS)
$ dig upc.edu +trace

Trobar respostes de resolvers DNS cau específics (p.ex. Cloudflare [1.1.1.1], UPC [147.83.0.1])
$ dig A www.upc.edu @1.1.1.1 +short

Trobar el temps de caducitat de la memòria cau (TTL) per a DNS RR
$ dig A www.upc.edu +nocmd +noall +answer +ttlid

3.3. El resolver

El *resolver* és una biblioteca que proporciona accés al DNS a qualsevol host. El seu fitxer de configuració "/etc/resolv.conf" conté informació per resoldre els noms contactant amb servidors DNS. Per exemple, si l'adreça d'un servidor DNS és 192.168.60.125:

```
root@aula01:/# cat /etc/resolv.conf
search xc.test
nameserver 192.168.60.125
```

on "nameserver" és l'adreça IP del servidor de noms local i "search" és el domini predeterminat per a les consultes. Si una resolució falla i hi ha diversos servidors de noms (diverses línies de "nameserver"), aquests es demanen seqüencialment. El domini predeterminat s'afegeix si el nom a resoldre no està totalment qualificat (complet).

3.4. El servidor Bind

Berkeley Internet Name Domain (BIND) és el programari de servidor DNS més popular. Depèn de dos tipus de fitxers per funcionar correctament: un fitxer de servidors arrel i un fitxer de zona.

El fitxer de servidors arrel, conté una llista de les adreces IP dels servidors DNS arrel a Internet. Aquests servidors proporcionen informació sobre els dominis de primer nivell (TLD) com .com, .net, .org, etc. Quan el servidor DNS BIND rep una sol·licitud d'un nom de domini que no té autoritat, consultarà els servidors arrel per determinar quins dels servidors arrel ha de consultar per obtenir l'adreça IP del següent nivell del nom de domini. Aquest fitxer a "/etc/bind/db.root" no s'ha de modificar. Forma part de la instal·lació de bind.

El fitxer de zona conté informació, registres de recursos (RR), sobre un domini (zona) per al qual és autoritzat un cert servidor DNS BIND. Aquest fitxer inclou registres que assignen noms de domini a adreces IP i altra informació com ara el servidor de correu i la informació del servidor de noms. El servidor DNS BIND utilitza aquesta informació per respondre a les consultes DNS d'aquest domini.

Per exemple, el fitxer db.grupX.xc del laboratori té la informació que es mostra a la figura següent. Tingueu en compte que aquest fitxer és una plantilla d'un fitxer de zona, on la X s'ha de canviar al valor corresponent, tal com s'explica a continuació. El tipus RR SOA (Start Of Authority) té paràmetres de configuración seguit d'altres RR.

```
@       IN      SOA     ns.grupX.xc.test hostmaster.grupX.xc.test (
                                1         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
        IN      NS      ns.grupX.xc.test.
        IN      MX      10 mail1.grupX.xc.test.
        IN      MX      20 mail2.grupX.xc.test.
;
ns.grupX.xc.test.    A       192.168.60.X ;Adreça IP del NS
mail1.grupX.xc.test. A       192.168.60.X ;Adreça IP del MX
mail2.grupX.xc.test. A       192.168.60.X ;Adreça IP del MX
www.grupX.xc.test.   CNAME   pcserver.grupX.xc.test.
smtp.grupX.xc.test.  CNAME   pcserver.grupX.xc.test.
pop3.grupX.xc.test.  CNAME   pcserver.grupX.xc.test.
pcserver.grupX.xc.test.      CNAME   pcX.grupX.xc.test.
pcX.grupX.xc.test.        A       192.168.60.X ;Adreça IP de PCX
```

4. Realització de la pràctica

L'objectiu de la pràctica és configurar una autoritat del subdomini grupX.xc.test d'un hipotètic domini xc.test, tal com mostra la Figura 37. A partir d'ara X és el nombre del PC que fa de servidor de noms. Per exemple, si aquest és 114, aleshores el subdonini serà grup114.xc.test. En un cas real existiria l'autoritat xc.test, que apuntaria cap a grupX.xc.test i seria accessible a través d'un root-server. Tenim un domini de prova grupX amb el seu servidor, i el servidor xc.test no existeix. Per tant, els noms de la zona no es poden resoldre des de la resta d'Internet.

Per tal de poder realitzar la pràctica oportunament, caldrà que cada grup d'estudiants utilitzi 2 PCs. Un que serà l'autoritat de **grupX**.xc.test, i un que farà de host d'aquest domini (**pcX.grupX**.xc.test) per a fer peticions, tal com mostra la figura.

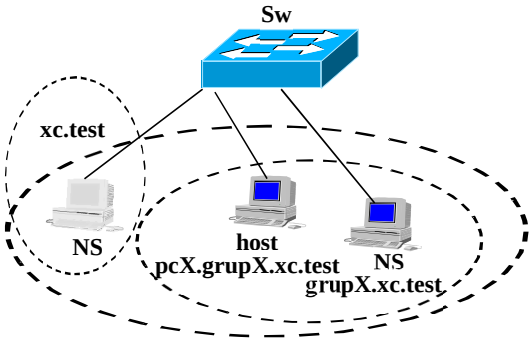


Figura 37. Xarxa a configurar. Només s'han de configurar pcX.grupX.xc.test i grupX.xc.test.

4.1. Configuració de la xarxa

1) Configurar els 2 PCs de la Figura 37 (el host pcX.grupX.xc i el servidor de noms grupX.xc.test) executant el client de dhcp (udhcpc). A continuació en pcX.grupX.xc.test executar "killall udhcpc", per matar el client de dhcp, altrament actualitzarà períodicanent el fitxer resolv.conf, esborrant els canvis que s'hagin fet al fitxer. A continuació modifiqueu el fitxer /etc/resolv.conf de pcX.grupX.xc.test perquè es faci servir el servidor de noms grupX.xc.test:

```
search grupX.xc.test
nameserver 192.168.?.?
```

on 192.168.?.? és l'adreça IP que el servidor de DHCP ha assignat al servidor de noms local grupX.xc.test.

4.2. Configuració del servidor de DNS de la subzona

Els fitxers de configuració es troben en la carpeta /home/xc/dns, que serà la carpeta de treball a partir d'ara.

2) Editar el fitxer 'named.conf' per indicar el domini i on es troba el fitxer de zona. Hi trobareu:

```
zone "grupX.xc.test" IN {
  type master;
  file "/home/xc/dns/db.grupX.xc";
};
```

On s'ha de canviar la X de `grupX.xc.test`. per el nombre del PC que es fa servir com a servidor de noms.

3) Modificar el fitxer 'db.grupX.xc'.canviant les X que calgui igual que abans (és a dir, amb el nombre del PC

que fa de servidor).

4) Un cop fet això, engegar el servidor de noms amb la comanda 'run_named.sh' com a root. Cal executar-ho cada cop que es modifiqui named.conf o db.grupX.xc. Comprova que està engegat executant "ps aux | egrep named". Si named no està corrent, mira si hi ha hagut errors executant: "tail –f /var/log/messages".

4.3. Observació del comportament del protocol DNS

5) Fent servir l'eina "dig" contesteu les següents preguntes. Quins registres heu consultat en cada ocasió? Assumiu que grupX i pcX són els corresponents al vostre grup:

   a. De quina màquina n'és àlies 'www.grupX.xc.test'?
   b. Quina és l'adreça IP del servidor 'www. grupX.xc.test'?
   c. Quins són els servidors de correu del domini 'grupX.xc.test'?

6) Engegueu el wireshark en l'equip que fa de servidor de DNS de la vostra zona per a fer captures del tràfic DNS que genereu, i observeu què passa quan es fan les peticions de l'apartat anterior. Navega a través dels camps dels paquets capturats per respondre el següent:

   a. Quants missatges es generen en cada resolució?
   b. És una resolució recursiva o iteractiva?
   c. Identifica les adreces de tots els servidors de noms que es consulten. S'ha fet servir algun root-server?
   d. Investiga el contingut dels camps (question, answer, authority, additional) de totes les respostes.

7) Captura el tràfic DNS que es genera quan es resol el nom www.microsoft.com. Navega a través dels camps dels paquets capturats ara per respondre el següent:

   a. Quants missatges es generen?
   b. És una resolució recursiva o interactiva?
   c. Identifica les adreces de tots els servidors de noms que es consulten. S'ha fet servir algun root-server?
   d. Investiga el contingut dels camps (question, answer, authority, additional) de totes les respostes enviades per els servidors.
   e. Quantes adreces IP representen el nom que s'ha resolt? Quins son els noms canònics de les adreces?

8) Fes servir la opció debug de dig (opció +trace). Repeteix la resolució de www.microsoft.com. Compara la informació proporcionada per dig amb el contingut dels missatges.

9) Canvieu el mode del vostre client (dig) a no recursiu (+norecurse). Què canvia quan ara repetiu la resolució de www.microsoft.com?

10) Prova de fer la resolució d'un nom configurat per un altre grup del laboratori. Quins missatges es generen? És possible fer la resolució? Perquè?

11) Obrir el navegador web i el wireshark en el host. Connecteu-vos a www.fib.upc.edu i observar les resolucions DNS que es generen.

5. Informe previ

1. Quins fitxers caldrà canviar de l'equip que faci de servidor de DNS de la subzona configurada en la pràctica?
2. Què és el mode recursiu i el mode iteratiu de DNS?
3. Quants missatges i quin contingut és d'esperar que es generin al fer la resolució del nom www.grupX.xc.test?
4. Quants missatges i quin contingut és d'esperar que es generin al fer la resolució del nom www.microsoft.com?