S4

Réseaux IP

Introduction aux services TCP/IP : DNS

Auteurs :
M. Samuel Riedo
M. Maic Queiroz

Encadrant :
M. François Buntschu

22 novembre 2016

Introduction

Le serveur DNS est un élément essentiel au fonctionnement d'Internet. Il a en effet la charge de traduire les noms de domaines en adresses IP et inversement. Il permet également d'assigner à un nom de domaine plusieurs adresses IP et permet ainsi de faire de la répartition de charge.
Dans ce laboratoire, nous allons tout d'abord mettre en place un serveur DNS puis analyser son fonctionnement à l'aide d'un analyseur réseau.

Problème 1

Documenter et valider le bon fonctionnement de votre maquette. Pour cela, utiliser les commandes *nslookup* et *ping* sur votre notebook.

La commande *nslookup* permet de trouver l'adresse IP associée à un nom de domaine. Pour google.ch, il s'agit de "172.217.16.131" ce qui est correct, car si nous entrons cette adresse dans un navigateur, le site google.ch est chargé.
Il est également possible de pinger l'adresse "8.8.8.8", ce qui correspond au serveur DNS de Google.
Enfin, il est possible de faire une requête DNS inverse pour trouver le nom de domaine associé à une adresse IP (toujours avec *nslookup*). Si nous tentons de trouver le nom de domaine de l'adresse "172.217.16.131", nous tombons sur google.com.

```
mbp-de-samuel-2:~ samuelriedo$ nslookup www.google.ch
Server:         160.98.30.206
Address:        160.98.30.206#53

Non-authoritative answer:
Name:   www.google.ch
Address: 172.217.16.131

mbp-de-samuel-2:~ samuelriedo$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=53 time=7.692 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=6.923 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=6.979 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=7.125 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=7.740 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=7.104 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.923/7.261/7.740/0.330 ms
mbp-de-samuel-2:~ samuelriedo$ nslookup 172.217.16.131
Server:         160.98.30.206
Address:        160.98.30.206#53

Non-authoritative answer:
131.16.217.172.in-addr.arpa     name = zrh04s06-in-f131.1e100.net.
131.16.217.172.in-addr.arpa     name = zrh04s06-in-f3.1e100.net.

Authoritative answers can be found from:
217.172.in-addr.arpa    nameserver = ns4.google.com.
217.172.in-addr.arpa    nameserver = ns3.google.com.
217.172.in-addr.arpa    nameserver = ns1.google.com.
217.172.in-addr.arpa    nameserver = ns2.google.com.
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
```

FIGURE 1 – nslookup & ping

Problème 2

Décrivez les différents paramètres de la configuration utilisés dans *db.pcltexx.ch.zone* et dans *db.30.98.160.in-addr.zone*.

```
$ORIGIN ltexx.ch.
$TTL 86400
@       IN      SOA     ltexx.ch.       root.ltexx.ch. (
                        2015111601      // serial number
                        3600            // refresh rate in second
                        900             // retry after 900s
                        604800          // expire after 604900s
                        86400 )         // negative cache

// Descriptions of names servers for this domain (primary and secondary)
                        // primary DNS
                        IN      NS      ourpc.ltexx.ch.
                        // secondary DNS
                        IN      NS      tlabs.tic.eia-fr.ch.

// List of known hosts in this domain
ourpc                   IN      A       160.98.30.206
www                     IN      CNAME   ourpc
smtp                    IN      CNAME   ourpc
pop                     IN      CNAME   ourpc
ltexx.ch.               IN      MX      10      pop.ltexx.ch.
```

Problème 3

Quels sont les paramètres qu'il faut configurer *au minimum* lorsque vous voulez gérer et configurer un domaine ?

Les paramètres du DNS ainsi que le serveur primaires sont obligatoires. Dans la liste des hosts connus, il faut au minimum le serveur primaire (ourpc dans ce cas).

```
$ORIGIN ltexx.ch.
$TTL 86400
@       IN      SOA     ltexx.ch.       root.ltexx.ch. (
                        2015111601      // serial number
                        3600            // refresh rate in second
                        900             // retry after 900s
                        604800          // expire after 604900s
                        86400 )         // negative cache

// Descriptions of names servers for this domain (primary and secondary)
                        // primary DNS
                        IN      NS      ourpc.ltexx.ch.

// List of known hosts in this domain
ourpc                   IN      A       160.98.30.206
```

Problème 4

Quel est l'organisme qui gère les domaines.ch ? Comment obtenez-vous cette information ?
L'organise qui gère les adresses ".ch" est Switch. Nous pouvons le savoir en tapant la commande *dig google.ch +trace*. Cette commande affiche tous les serveurs consultés lors d'une requête DNS.

```
mbp-de-samuel-2:~ samuelriedo$ dig google.ch +trace

; <<>> DiG 9.8.3-P1 <<>> google.ch +trace
;; global options: +cmd
.                       517144  IN      NS      g.root-servers.net.
.                       517144  IN      NS      f.root-servers.net.
.                       517144  IN      NS      d.root-servers.net.
.                       517144  IN      NS      m.root-servers.net.
.                       517144  IN      NS      l.root-servers.net.
.                       517144  IN      NS      e.root-servers.net.
.                       517144  IN      NS      j.root-servers.net.
.                       517144  IN      NS      i.root-servers.net.
.                       517144  IN      NS      h.root-servers.net.
.                       517144  IN      NS      b.root-servers.net.
.                       517144  IN      NS      a.root-servers.net.
.                       517144  IN      NS      c.root-servers.net.
.                       517144  IN      NS      k.root-servers.net.
;; Received 508 bytes from 160.98.30.206#53(160.98.30.206) in 180 ms

ch.                     172800  IN      NS      b.nic.ch.
ch.                     172800  IN      NS      h.nic.ch.
ch.                     172800  IN      NS      c.nic.ch.
ch.                     172800  IN      NS      f.nic.ch.
ch.                     172800  IN      NS      e.nic.ch.
ch.                     172800  IN      NS      a.nic.ch.
ch.                     172800  IN      NS      d.nic.ch.
;; Received 451 bytes from 192.36.148.17#53(192.36.148.17) in 847 ms

google.ch.              3600    IN      NS      ns1.google.com.
google.ch.              3600    IN      NS      ns2.google.com.
google.ch.              3600    IN      NS      ns3.google.com.
google.ch.              3600    IN      NS      ns4.google.com.
;; Received 109 bytes from 85.119.5.230#53(85.119.5.230) in 115 ms

google.ch.              300     IN      A       172.217.19.3
;; Received 43 bytes from 216.239.38.10#53(216.239.38.10) in 21 ms
```

FIGURE 2 – Résolution DNS

La première étape consiste à consulter les serveurs root pour trouver quels serveurs DNS gèrent la branche ".ch". Une fois ceci fait, ces derniers serveurs vont être consultés pour trouver *google.ch*. À ce moment, nous pouvons voir que les serveurs "nic.ch" sont consultés. Si nous tapons ceci dans un navigateur, nous arrivons sur le site "Switch.ch".

Problème 5

À quoi sert le fichier *./etc/bind/db.root* ?
Il contient l'adresse IP de chacun des 13 serveurs root. C'est le point de départ de toute requête DNS. Ces adresses étant statiques, elles peuvent être stockées.

Problème 6

Quels sont les protocoles de couche 2, 3 et 4 utilisés pour l'échange DNS ? Indiquez le champ dans chacune des couches qui vous permet de définir le protocole qui est transporté.
Comme ont peut le voir dans wireshark, les protocoles utilisés (encadré en rouge) sont :

— **deuxième couche :** Ethernet II
— **troisième couche :** IPv4
— **quatrième couche :** UDP

Les champs utilisés dans chacune des couches sont encadrés en bleu dans l'image ci-dessous :

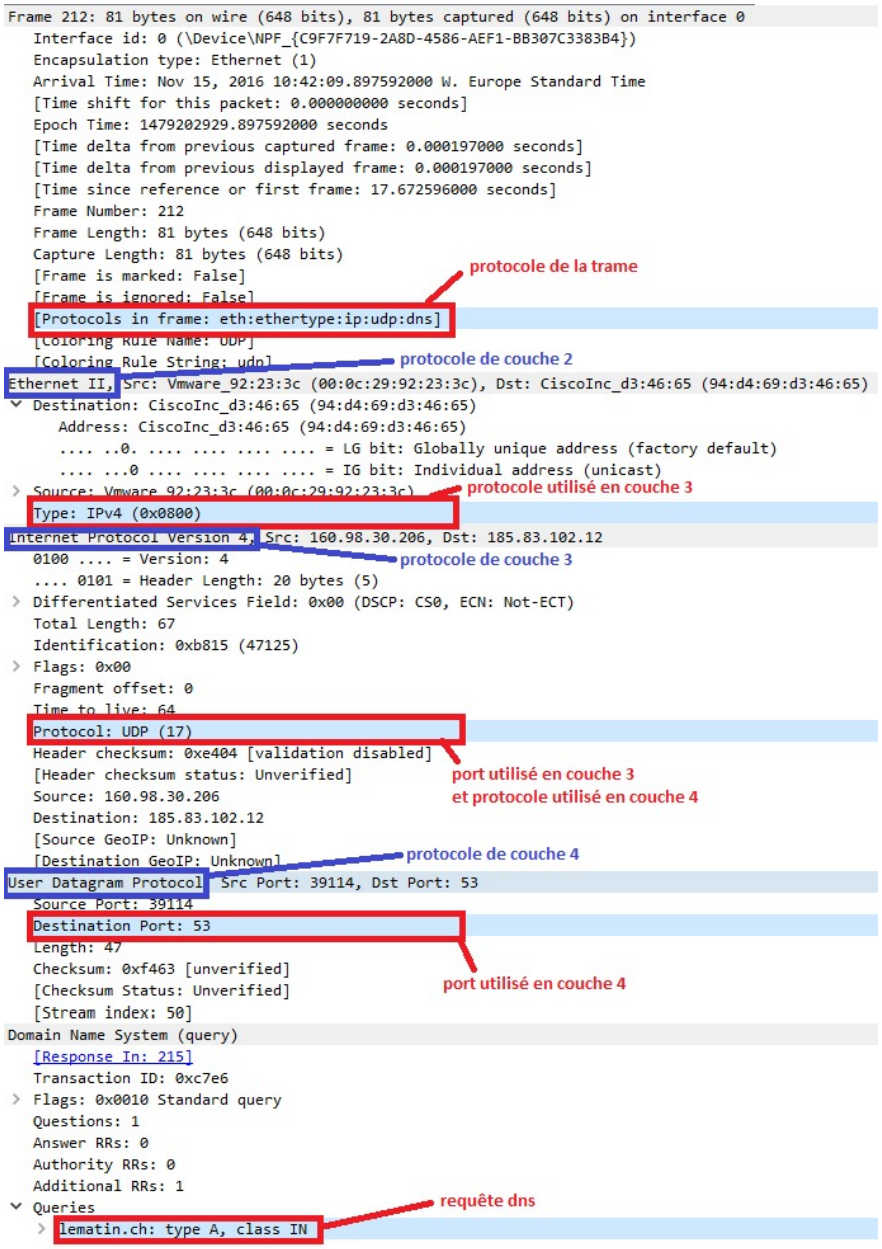

FIGURE 3 – Trame dans Wireshark

Problème 7

Quels sont les interlocuteurs de votre notebook et de la machine Linux pour les dialogues DNS ? Quelles sont leurs adresses IP ? Combien de trames provenant et à destination de votre notebook avez-vous enregistrées ? Commentez.
Le notebook a un seul interlocuteur, il s'agit de notre machine Linux.
Adresse IP : 160.98.30.206 **Adresse MAC :** 00 : 0c : 29 : 92 : 23 : 3c
Les interlocuteurs de notre machine Linux sont un plus nombreux. Nous avons par exemple :
Adresse IP : 185.83.102.12 **Adresse MAC :** 94 : d4 : 69 : d3 : 46 : 65

Nous avons enregistré une multitude de trames en provenance et à destination de notre notebook. Elles sont toujours par paire. En effet, il y a une requête en IPv4 (A) et une autre en IPv6 (AAAA) ainsi que leurs réponses respectives. De plus, si le site sur lequel nous nous rendons (dans notre cas lematin.ch) contient des liens vers d'autres sites, des requêtes supplémentaires seront faites pour résoudre également ces noms de domaine.

Problème 8

Quels sont les types de messages DNS observés ?
Il y a 2 types de messages DNS. Le *standard query* qui est la requête DNS et le *standard query response* qui est la réponse à cette requête.

→	504	55.510159	160.98.30.26	160.98.2.110	DNS	84 Standard query 0xdce0 A hefrsccm01.sofr.hefr.lan
	505	55.510444	160.98.30.26	160.98.2.110	DNS	84 Standard query 0xa1f7 AAAA hefrsccm01.sofr.hefr.lan
←	506	55.511340	160.98.2.110	160.98.30.26	DNS	100 Standard query response 0xdce0 A hefrsccm01.sofr.hefr.lan A 160.98.2.63
	507	55.511352	160.98.2.110	160.98.30.26	DNS	147 Standard query response 0xa1f7 AAAA hefrsccm01.sofr.hefr.lan SOA hefrns01.hefr.ch

FIGURE 4 – Trames échangées entre le PC et le serveur DNS

Problème 9

Dessinez les échanges observés entre le client, le serveur DNS et Internet en fonction du temps (diagramme en flèche), commentez.
Nous avons pu remarquer a l'aide du diagramme en flèches que la requête est de type récursif. Notre serveur fait donc les requêtes de manière itérative afin de nous fournir une réponse complète et terminée.

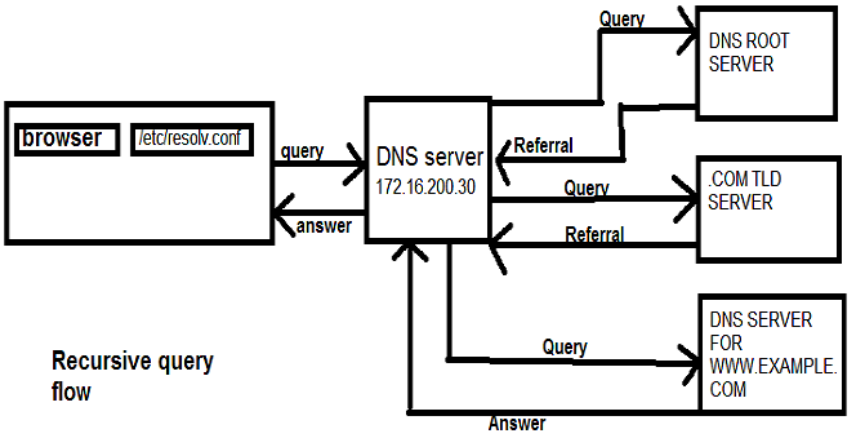

FIGURE 5 – Principe de fonctionnement d'une requête récursive

Nous avons généré le diagramme en flèches sur wireshark mais compte tenu du nombre de noeuds, il est impossible de le mettre en entier pour des raisons de lisibilité. Il est cependant composé de 9 noeuds pour 14 échanges. Et comme la requête est de type récursif, nous avons que 2 trames échangées entre notre PC et le serveur.

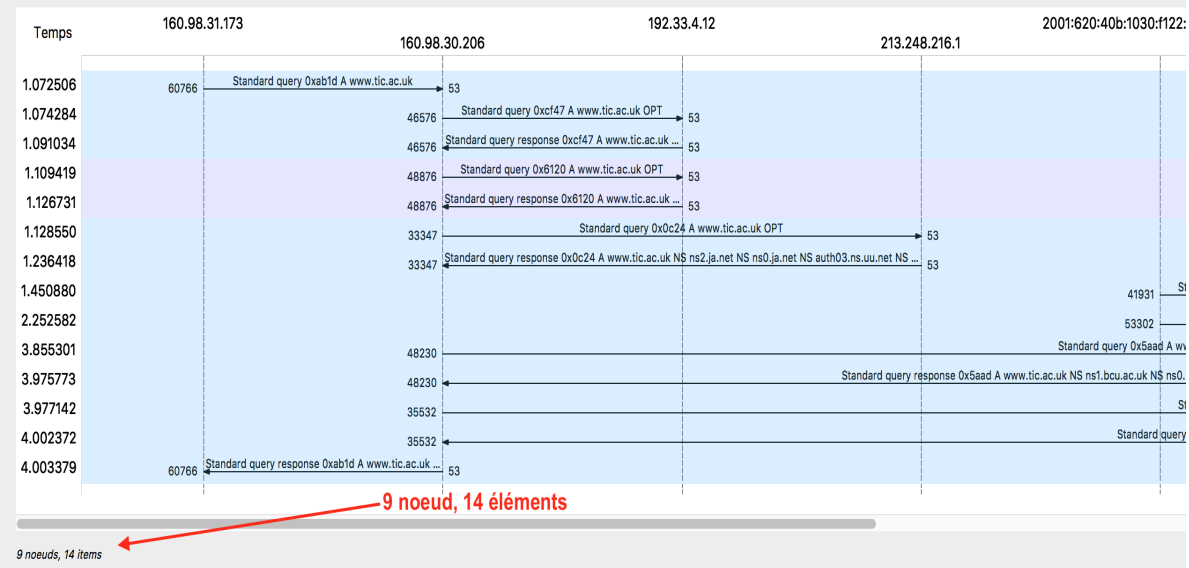

FIGURE 6 – Trames échangées entre le PC, le serveur DNS et internet

Problème 10

Où se trouve l'information demandée ? Quelles sont les réponses du serveur DNS ?
DNS étant un protocole couche 5, c'est dans cette même couche que se trouvera le nom de domaine de la requête (figure 3).

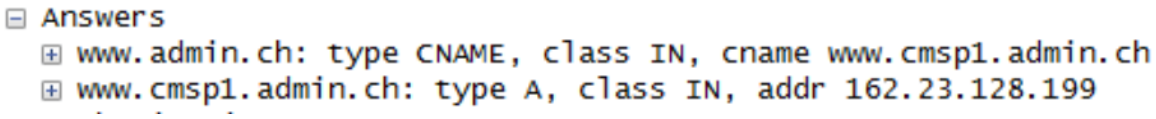

FIGURE 7 – Requête DNS

Le champ *querie* contient le nom de domaine *admin.ch*. Étant de type *CNAME*, il s'agit d'un alias de *cmsp1.admin.ch*. L'IP de ce domaine est *162.23.128.199*.

Problème 11

Quels sont les types de messages DNS observés ?
Les messages sont les mêmes que pour une requête non inverse, c'est-à-dire *standard query* et *standard query response*.

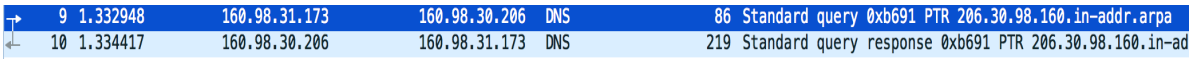

FIGURE 8 – Requête DNS inverse

Problème 12

Où se trouve l'information demandée ? Quelles sont les réponses du serveur DNS ?
La demande d'information se trouve dans le champ *querie* de la demande DNS. Ci-dessous, une demande sur l'adresse *206.30.98.160.in-addr.arpa* de type PTR (Pointer to a canonical name, c'est-à-dire pas un alias).

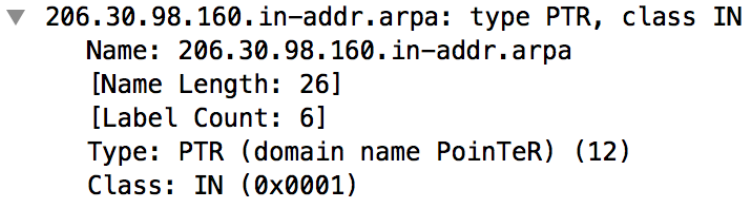

FIGURE 9 – Demande DNS inverse

Identiquement aux requêtes non inverse, l'information de la réponse se trouve dans le champ *answer*. Cette réponse contient également la liste des serveurs autoritaire pour ce domaine, soit notre serveur DNS *ourpc.lte06.ch* et le serveur DNS de l'école *tlabs.tic.eia-fr.ch*.

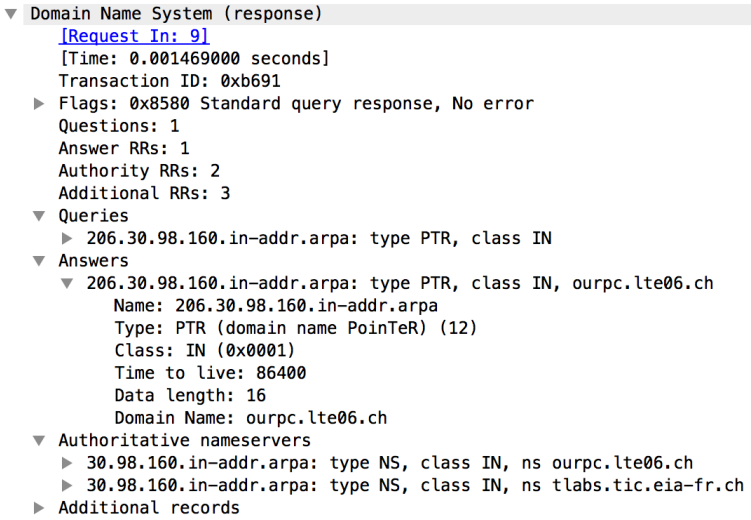

FIGURE 10 – Réponse DNS inverse

Problème 13

Dessiner le diagramme en flèches des échanges observés.
Nous avons réalisé le diagramme en flèche sur wireshark, cependant, compte tenu du nombre de noeuds, il est impossible de mettre le graphique complet pour des raisons de lisibilité. Il est cependant composé de 9 noeuds pour 14 échanges.

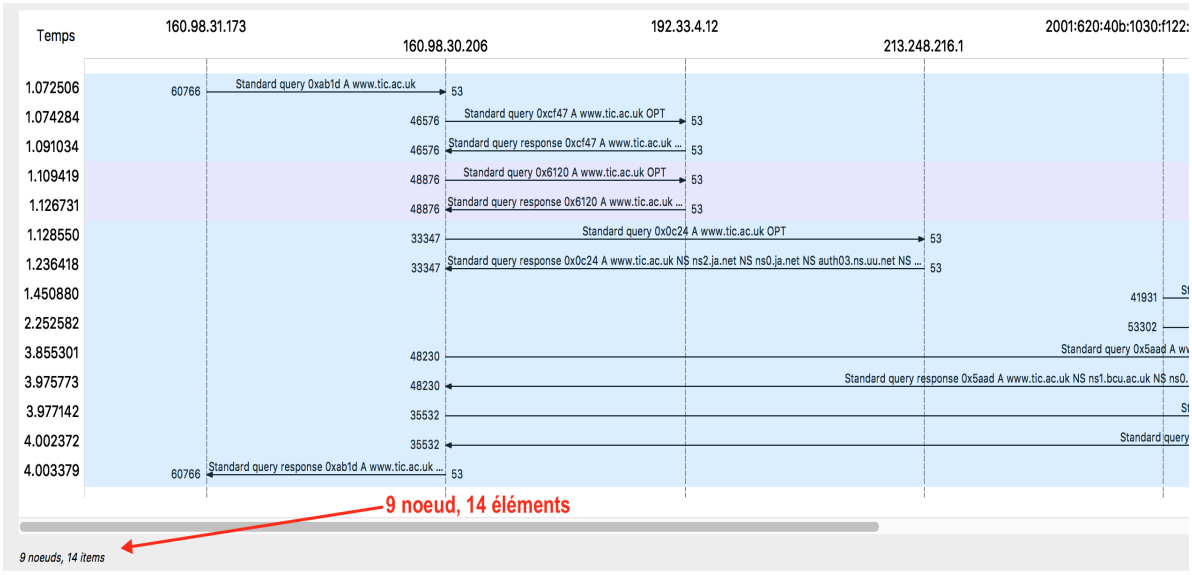

FIGURE 11 – Trames échangées entre le PC, le serveur DNS et internet

Problème 14

Combien de requêtes effectue votre serveur DNS pour résoudre la requête ci-dessus ?
Nous avons eu 8 requêtes et 6 réponses lors de la résolution du nom "www.tic.ac.uk".

dns.qry.name contains "tic.ac.uk"

No.	Time	Source	Destination	Protocol	Length	Info
87	1.072506	160.98.31.173	160.98.30.206	DNS	73	Standard query 0xab1d A www.tic.ac.uk
88	1.074284	160.98.30.206	192.33.4.12	DNS	84	Standard query 0xcf47 A www.tic.ac.uk OPT
91	1.091034	192.33.4.12	160.98.30.206	DNS	84	Standard query response 0xcf47 A www.tic.ac.uk OPT
98	1.109419	160.98.30.206	192.33.4.12	DNS	110	Standard query 0x6120 A www.tic.ac.uk OPT
101	1.126731	192.33.4.12	160.98.30.206	DNS	865	Standard query response 0x6120 A www.tic.ac.uk NS c
105	1.128550	160.98.30.206	213.248.216.1	DNS	84	Standard query 0x0c24 A www.tic.ac.uk OPT
115	1.236418	213.248.216.1	160.98.30.206	DNS	462	Standard query response 0x0c24 A www.tic.ac.uk NS r
533	1.450880	2001:620:40b:1030:…	2001:630:0:45::11	DNS	104	Standard query 0x7766 A www.tic.ac.uk OPT
601	2.252582	2001:620:40b:1030:…	2001:630:0:8::14	DNS	104	Standard query 0xa7b2 A www.tic.ac.uk OPT
762	3.855301	160.98.30.206	198.6.1.83	DNS	84	Standard query 0x5aad A www.tic.ac.uk OPT
768	3.975773	198.6.1.83	160.98.30.206	DNS	395	Standard query response 0x5aad A www.tic.ac.uk NS r
769	3.977142	160.98.30.206	193.60.130.118	DNS	84	Standard query 0x37d8 A www.tic.ac.uk OPT
771	4.002372	193.60.130.118	160.98.30.206	DNS	100	Standard query response 0x37d8 A www.tic.ac.uk A 19
772	4.003379	160.98.30.206	160.98.31.173	DNS	161	Standard query response 0xab1d A www.tic.ac.uk A 19

FIGURE 12 – Trames échangées lors de la résolution DNS

Conclusion

Comme nous avons pu le constater, le serveur DNS est très utile sur internet et dans les réseaux locaux. Il permet de simplifier la vie des utilisateurs, car, en effet, il serait tout simplement impossible de retenir des milliers d'adresses IP correspondants à des sites ou des machines locales. Les noms sont plus facilement mémorisables qu'une série de chiffres (en IPV4) ou qu'une série de chiffre et de lettres (en IPV6).
Nous avons cependant eu quelques soucis au début du TP à obtenir les captures désirées. En effet, il est important de vider le cache DNS sur le client ainsi que sur le serveur avant de faire les mesures sous peine de biaiser les résultats.

Table des figures

Fribourg, le 22 novembre 2016

Samuel Riedo

Maic Queiroz