



Haute école d'ingénierie et d'architecture Fribourg  
Hochschule für Technik und Architektur Freiburg

Réseaux IP

Rapport de travail pratique

# **Bridging & Spanning-Tree**

*Auteur :*

Josué Tille, Marc Roten

2 décembre 2017

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Configuration d'expérience</b>	<b>2</b>
<b>3</b>	<b>Protocole DNS</b>	<b>6</b>
3.1	Analyse des protocoles observés . . . . .	6
3.2	Analyse des échanges DNS . . . . .	8
<b>4</b>	<b>Conclusion</b>	<b>9</b>

# 1 Introduction

Ce travail pratique a pour but de nous introduire aux services TCP/IP, plus particulièrement le protocole DNS, qui est omniprésent, dans notre vie de tous les jours. Effectivement c'est plus facile de se souvenir d'un nom de domaine comme tlabs.tic.heia-fr.ch plutôt que 160.98.31.32.

## 2 Configuration d'expérience

**P1:** Documenter et valider le bon fonctionnement de votre maquette. Pour cela, utiliser les commandes "nslookup" et "ping" sur votre notebook.

Dans un premier temps il est nécessaire de vérifier une bonne configuration du réseau. Pour cela nous avons procédé à un ping du serveur DNS qui permet de valider que l'adressage IP et que les routes sont corrects :

```
# ping 160.98.30.207
PING 160.98.30.207 (160.98.30.207) 56(84) bytes of data.
64 bytes from 160.98.30.207: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 160.98.30.207: icmp_seq=2 ttl=64 time=0.963 ms
64 bytes from 160.98.30.207: icmp_seq=3 ttl=64 time=0.868 ms
64 bytes from 160.98.30.207: icmp_seq=4 ttl=64 time=0.959 ms
```

Suite à ce test nous avons pu vérifier le bon fonctionnement de notre serveur DNS. Pour cela nous avons utilisé la commande "dig" qui permet d'avoir plus d'informations que nslookup. Pour commencer nous avons testé la bonne résolution de "ourpc.lte07.ch" :

```

→ ~ dig @160.98.30.207 ourpc.lte07.ch

; <<> DiG 9.10.3-P4-Ubuntu <<> @160.98.30.207 ourpc.lte07.ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1263
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;ourpc.lte07.ch.                IN      A

;; ANSWER SECTION:
ourpc.lte07.ch.                86400   IN      A      160.98.31.170

;; AUTHORITY SECTION:
lte07.ch.                      86400   IN      NS      ourpc.lte07.ch.
lte07.ch.                      86400   IN      NS      tlabs.tic.eia-fr.ch.

;; ADDITIONAL SECTION:
tlabs.tic.eia-fr.ch.          85548   IN      A      160.98.31.32
tlabs.tic.eia-fr.ch.          85548   IN      AAAA    2001:620:40b:1030::a062:1f20

;; Query time: 2 msec
;; SERVER: 160.98.30.207#53(160.98.30.207)
;; WHEN: Wed Nov 29 14:35:33 CET 2017
;; MSG SIZE rcvd: 148

```

Figure 1 – Capture de la commande dig depuis une des machines clientes

On peut donc constater que dans la section “ANSWER” on a la réponse à notre question qui est “160.98.31.170”.

**P2:** Décrivez les différents paramètres de configurations utilisés dans db.pclte07.ch.zone et dans le db.30.98.160.in-addr.zone

```

; Haute ecole d'ingenierie et d'architecture de Fribourg
; Reseaux IP
; -----
; TP DNS - Filename= ltexx.ch.zone
; -----
; (c) F. Buntschu
;
; Version 1.4
; -----
$ORIGIN lte07.ch.
$TTL 86400
@ IN SOA lte07.ch. root.lte07.ch. (
    2015111601
    3600
    900
    604800
    86400 )

; Descriptions of names servers for this domain (primary and secondary)
    IN NS ourpc.lte07.ch.
    IN NS tlabz.tic.eia-fr.ch.

; List of known hosts in this domain
ourpc      IN A 160.98.31.170
www        IN CNAME ourpc
smtp       IN CNAME ourpc
pop        IN CNAME ourpc
lte07.ch.  IN MX 10 pop.lte07.ch.
  
```

Figure 2 – Capture de la commande dig depuis une des machines clientes

Le fichier de configuration `db.pclte07.ch.zone` contient toutes les informations concernant le domaine `lte07.ch`. Le `ORIGIN` contiendra le nom de la zone en question puis le `TTL` contiendra la durée par défaut en secondes pendant laquelle les caches pourront considérer cette information comme valide. Par exemple si un contien une entrée DNS ayant un TTL de 60. Le cache devra, si il a des requête demandant ce nom de domaine, redemander ce nom toutes les 60 secondes.

Ensuite dans ce fichier nous aurons les entrée DNS suivantes :

**SOA (Start Of Authority)** Cette entrée contiendra principalement des informations concernant le propriétaire de la zone et des informations utiles pour les serveur esclaves. Il y aura notamment : le nom de la zone et l'adresse email de l'administrateur. Pour les serveur secondaires il y aura :

- Le numéro de série (permettant aux serveur de savoir si la zone à changé). Ce numéro devra être incrémenté à chaque modification dans la zone.
- Les valeurs suivantes sont des surée en secondes indiquant aux serveur secondaire la durée de rafraichissement de la zone, les temps d'expiration, etc.

**NS** Ces 2 entrée contiendrons l'adresse des serveurs qui ont autorité pour la zone en question. On a donc ici notre serveur DNS `ourpc.lte07.ch.` et aussi le serveur `tlabz.tic.eia-fr.ch.` qui a aussi autorité pour la zone en question. Cela implique que un résolveur peut s'adresser à l'un ou l'autre des serveur pour connaitre des informations sur la zone.

**A** Cette entrée contiendra toujours une IPv4. Ici nous indiquons l'adresse ip de la machine `ourpc.lte07.ch.`

**CNAME** Cette entrée permet d'associer plusieurs noms DNS pour la même entrée A, AAAA, MX, etc. Dans ce cas cela l'entrée `www IN CNAME ourpc` implique que `www` est identique à `ourpc`.

**MX** Cette entrée sera utilisée uniquement pour la messagerie. Cela indique le nom de domaine du serveur mail associé à la zone en question.

Dans le fichier de zone `db.30.98.160.in-addr.zone` nous aurons les mêmes entrée SOA et NS que dans `db.pclte07.ch.zone`. Au lieu d'avoir des entrée CNAME, A nous aurons des entrée PTR. Ce type d'entrée est en quelque sorte l'inverse de l'entrée A. Elle contiendra une partie d'adresse IP qui pointera vers un nom de domaine.

**P3:** Quels sont les paramètres qu'il faut configurer au minimum lorsque vous voulez gérer et configurer un domaine.

Les éléments minimum sont les suivants :

**SOA** Une zone a besoin d'un enregistrement SOA pour définir qui fait autorité sur la zone.

**NS** Il est obligatoire de définir à quel serveur s'adresse pour obtenir des information sur la zone.

**P4:** Quel est l'organisme qui gère les domaines `.ch`? Comment obtenez-vous cette information?

C'est switch. Il existe plusieurs moyens d'obtenir cette information, notamment en cherchant sur internet. Ici nous allons utiliser la commande `whois` qui permet d'obtenir toutes les informations concernant le propriétaire de la zone en question :

```
# whois ch
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:          CH

organisation: SWITCH The Swiss Education & Research Network
address:         Werdstrasse 2
address:         Zurich CH-8021
address:         Switzerland

contact:         administrative
name:            SWITCH TLD Administration
organisation: SWITCH The Swiss Education & Research Network
address:         Werdstrasse 2
address:         Zurich CH-8021
address:         Switzerland
phone:           +41 44 268 15 40
fax-no:          +41 44 268 15 78
e-mail:          tld-admin@switch.ch

contact:         technical
name:            Security Engineer
organisation: SWITCH The Swiss Education & Research Network
address:         Werdstrasse 2
address:         Zurich CH-8021
address:         Switzerland
phone:           +41 44 268 15 40
fax-no:          +41 44 268 15 78
e-mail:          dns-operation@switch.ch
```

Figure 3 – Retour de la commande whois

Comme on peut le constater SWITCH est l'organisation qui gère Techniquement et Administrativement la zone .ch.

**P5:** A quoi sert le fichier /etc/bind/db.root?

Ce fichier permet au résolveur DNS de connaître l'adresse IP des serveurs Racines. Étant donné que la structure DNS est en arbre, pour commencer la résolution on doit savoir où atteindre la Racine de notre arbre. Ce Type de donnée est obligatoire pour tout résolveurs DNS, sinon aucune résolution sera possible.

## 3 Protocole DNS

### 3.1 Analyse des protocoles observés

**P6:** 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.

```
Frame 7: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
-Ethernet II, Src: Dell_31:25:01 (5c:26:0a:31:25:01), Dst: Cisco_d3:46:65 (94:d4:69:d3:46:65)
-Internet Protocol Version 4, Src: 160.98.31.181, Dst: 160.98.30.207
-User Datagram Protocol, Src Port: 56010, Dst Port: 53
-Domain Name System (query)
```

Figure 4 – Capture d'une requête DNS

Comme on peut le constater dans l'illustration 7 on peut voir que en couche 2 nous avons une trame de protocole Ethernet, ensuite nous avons en couche 3 le protocole IP qui est utilisé. En couche 4 nous aurons UDP qui est utilisé.

**P7:** 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 enregistré? Commentez!

267 3.098595246	160.98.31.181	160.98.30.207	DNS	72 Standard query 0xc462 A www.admin.ch
391 3.586476773	160.98.31.181	160.98.30.207	DNS	71 Standard query 0xc0dc A tv.admin.ch
392 3.586501150	160.98.31.181	160.98.30.207	DNS	71 Standard query 0x4db0 AAAA tv.admin.ch
393 3.587076604	160.98.31.181	160.98.30.207	DNS	71 Standard query 0xc0dc A tv.admin.ch
394 3.587091666	160.98.31.181	160.98.30.207	DNS	71 Standard query 0x4db0 AAAA tv.admin.ch
3681 6.286840525	160.98.30.207	194.0.1.40	DNS	83 Standard query 0xc445 A www.admin.ch OPT
2643 6.387071418	160.98.30.207	194.0.1.40	DNS	82 Standard query 0x3f70 AAAA www.admin.ch OPT
3734 6.322869253	194.0.1.40	160.98.30.207	DNS	140 Standard query response 0xc445 A www.admin.ch NS ins1.admin.ch NS ins2.admin.ch NS ins3.admin.ch OPT
3735 6.322879455	194.0.1.40	160.98.30.207	DNS	140 Standard query response 0x3f70 AAAA www.admin.ch NS ins1.admin.ch NS ins2.admin.ch NS ins3.admin.ch OPT
3808 6.394733645	160.98.30.207	194.0.1.40	DNS	109 Standard query 0xd5ac A www.admin.ch OPT
3801 6.394928392	160.98.30.207	194.0.1.40	DNS	109 Standard query 0xef1f AAAA www.admin.ch OPT
3823 6.412790543	194.0.1.40	160.98.30.207	DNS	797 Standard query response 0xd5ac A www.admin.ch NS ins1.admin.ch NS ins2.admin.ch NS ins3.admin.ch NSSEC R...
3826 6.413538104	194.0.1.40	160.98.30.207	DNS	797 Standard query response 0xef1f AAAA www.admin.ch NS ins1.admin.ch NS ins2.admin.ch NS ins3.admin.ch NSSEC
3828 6.413509959	160.98.30.207	212.193.72.85	DNS	83 Standard query 0x1401 A www.admin.ch OPT
3832 6.414072077	160.98.30.207	212.193.72.85	DNS	83 Standard query 0xbfb0 AAAA www.admin.ch OPT
3837 6.423556374	212.193.72.85	160.98.30.207	DNS	123 Standard query response 0x1401 A www.admin.ch CNAME www.cmspl.admin.ch A 162.23.128.199 OPT
3838 6.424045378	212.193.72.85	160.98.30.207	DNS	158 Standard query response 0xbfb0 AAAA www.admin.ch CNAME www.cmspl.admin.ch SOA ins1.admin.ch OPT
3842 6.424918791	160.98.30.207	162.23.37.16	DNS	89 Standard query 0x1a84 A www.cmspl.admin.ch OPT
3843 6.425229989	160.98.30.207	162.23.37.16	DNS	89 Standard query 0x2622 AAAA www.cmspl.admin.ch OPT
3849 6.448056469	162.23.37.16	160.98.30.207	DNS	140 Standard query response 0x1a84 A www.cmspl.admin.ch A 162.23.128.199 OPT
3847 6.434182125	162.23.37.16	160.98.30.207	DNS	140 Standard query response 0x2622 AAAA www.cmspl.admin.ch SOA ins1.admin.ch OPT
3848 6.434713335	160.98.30.207	160.98.31.181	DNS	217 Standard query response 0xbfb0 A www.admin.ch CNAME www.cmspl.admin.ch A 162.23.128.199 NS ins2.admin.ch...
3849 6.435067662	160.98.30.207	160.98.31.181	DNS	217 Standard query response 0xc462 A www.admin.ch CNAME www.cmspl.admin.ch A 162.23.128.199 NS ins1.admin.ch...
3850 6.435179615	160.98.30.207	160.98.31.181	DNS	147 Standard query response 0xffff AAAA www.admin.ch CNAME www.cmspl.admin.ch SOA ins1.admin.ch
3882 6.557067256	160.98.31.181	160.98.30.207	DNS	84 Standard query 0x4cb2 A www.ces-etcourt.admin.ch
3883 6.557031830	160.98.31.181	160.98.30.207	DNS	84 Standard query 0x4cb2 A www.ces-etcourt.admin.ch
3884 6.558456470	160.98.30.207	162.23.37.160	DNS	95 Standard query 0x58a3 A www.ces-etcourt.admin.ch OPT

Figure 5 – Capture de toutes les requêtes effectuée lors de la consultation de la page "www.admin.ch" - En Bleu : Requetes PC <-> Résolveur DNS, En rose : Requetes Résolveur DNS <-> serveur authoritative pour .ch, En Vert : Résolveur DNS <-> Serveur authoritative pour admin.ch

On peut remarquer que au début le notre PC enverra une requête au serveur DNS pour connaître l'adresse ip pour le domaine www.admin.ch. Ensuite le serveur effectuera tout le processus de résolution avant d'envoyer finalement la réponse au client. Dans ce processus il contactera dans notre cas le serveur à l'adresse 194.0.1.40. Cette adresse ip correspond au serveur DNS de switch pour la zone .ch (vérifié avec la commande "host -t PTR 194.0.1.40"). Lors de cette requête nous avons constaté que il envoie une première fois la requête en UDP puis ensuite il la renvoie en TCP (Requêtes en rose). Pour terminer il enverra plusieurs requête aux serveur serveur authoritative de admin.ch (ip 212.193.72.85, 162.23.37.16).

Nous avons constaté que dans ces requêtes nous avons pas de communication avec les root serveur. Cela est probablement du au fait que l'adresse des serveur authoritative pour .ch était déjà dans le cache de notre résolveur (malgré un restart du serveur avant la capture).



## 3.2 Analyse des échanges DNS

**P8:** Quels sont les types de message DNS observés ?

Nous avons observé 2 types de messages DNS. Les requêtes et les réponses. Nous avons aussi observé l'utilisation de 2 protocoles de transport soit UDP et TCP pour le DNS.

```

> Frame 2505: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
> Ethernet II, Src: Cisco_a3:46:65 (94:04:69:d3:46:65), Dst: PcsCompu_46:1e:ac (08:00:27:46:1e:ac)
> Internet Protocol Version 4, Src: 194.0.17.1, Dst: 160.98.30.207
> User Datagram Protocol, Src Port: 53, Dst Port: 60096
> Domain Name System (response)

> Frame 2048: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
> Ethernet II, Src: PcsCompu_46:1e:ac (08:00:27:46:1e:ac), Dst: Cisco_a3:46:65 (94:04:69:d3:46:65)
> Internet Protocol Version 4, Src: 160.98.30.207, Dst: 194.0.17.1
> Transmission Control Protocol, Src Port: 40195, Dst Port: 53, Seq: 1, Ack: 1, Len: 44
> Domain Name System (query)

```

Figure 6 – Observation 2 requêtes DNS avec les 2 protocoles de transport

**P9:** Dessinez les échanges observés entre le client, le serveur DNS et Internet en fonction du temps, commentez !

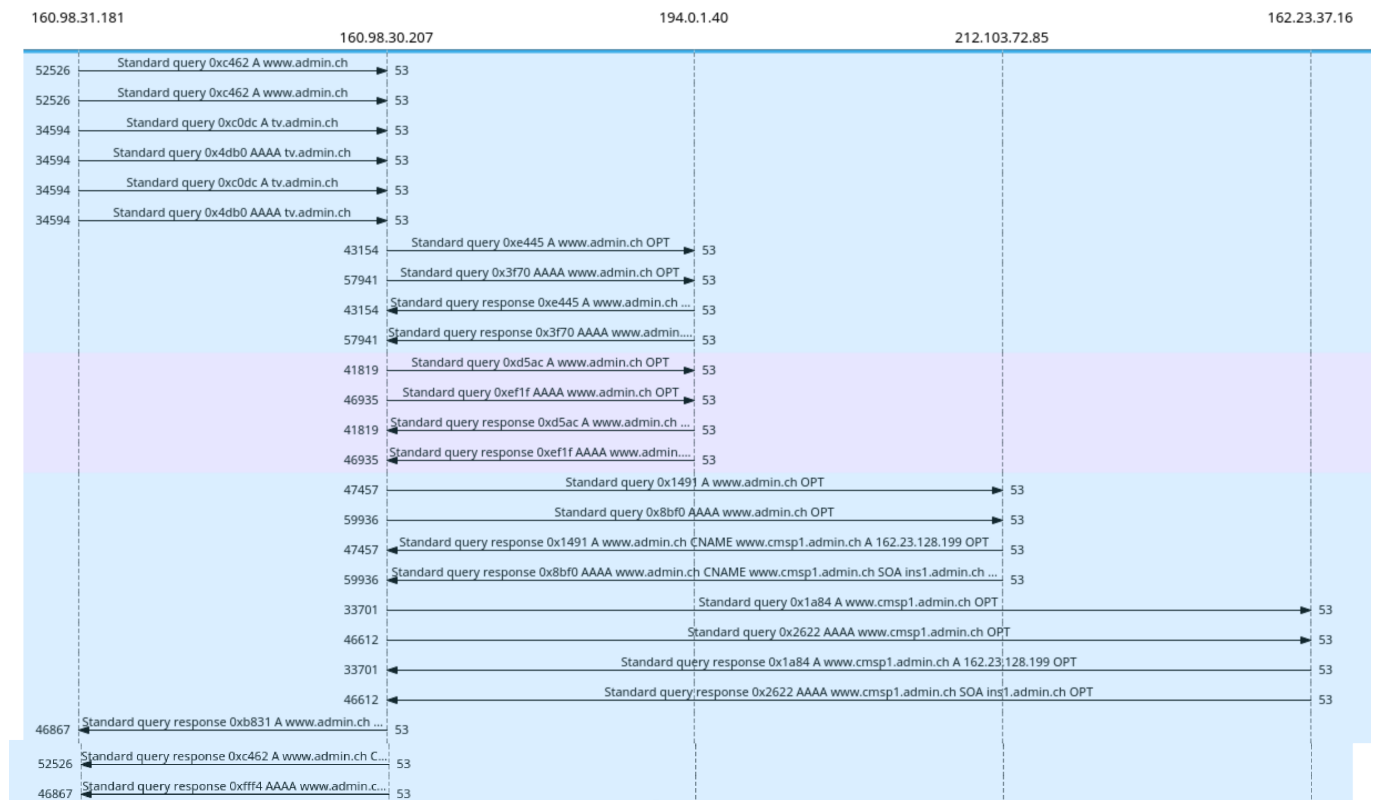


Figure 7 – Digramme en flèches de la requête DNS www.admin.ch depuis notre notebook.

**P10:** Où se trouve l'information demandée ? Quelles sont les réponses du serveur DNS ?

**P11:** Quels sont les types de message DNS observés ?

Ici étant donné que nous voulons savoir quel est le nom de domaine lié à 160.98.30.207 il s'agit d'une requête DNS inverse. Les types de message seront très semblables aux précédentes : Une requête et une réponse. Seule différence si on analyse la requête DNS on peut observer que la question est l'enregistrement PTR de 170.30.98.160.in-addr.arpa au lieu d'un enregistrement A.

```

> Frame 242: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
> Ethernet II, Src: Cisco_d3:46:65 (94:d4:69:d3:46:65), Dst: PcsCompu_46:1e:ac (08:00:27:46:1e:ac)
> Internet Protocol Version 4, Src: 160.98.31.181, Dst: 160.98.30.207
> User Datagram Protocol, Src Port: 36716, Dst Port: 53
> Domain Name System (query)
  [Response In: 243]
  - Transaction ID: 0x0989
  - Flags: 0x0120 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 1
  - Queries
    > 170.30.98.100.in-addr.arpa: type PTR, class IN
  - Additional records

> Frame 243: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0
> Ethernet II, Src: PcsCompu_46:1e:ac (08:00:27:46:1e:ac), Dst: Dell_31:25:01 (5c:20:0a:31:25:01)
> Internet Protocol Version 4, Src: 160.98.30.207, Dst: 160.98.31.181
> User Datagram Protocol, Src Port: 53, Dst Port: 36716
> Domain Name System (response)
  [Request In: 242]
  - [Time: 0.00064436 seconds]
  - Transaction ID: 0x0989
  - Flags: 0x8580 Standard query response, No error
  - Questions: 1
  - Answer RRs: 1
  - Authority RRs: 2
  - Additional RRs: 4
  - Queries
    > 170.30.98.100.in-addr.arpa: type PTR, class IN
  - Answers
    > 170.30.98.100.in-addr.arpa: type PTR, class IN, ourpc.lte07.ch
  - Authoritative nameservers
  - Additional records
  
```

Figure 8 – Vue détaillé de la requête et de la réponse

**P12:** Où se trouve l'information demandée? Quelles sont les réponses du serveur DNS?

Le serveur n'aura pas besoin de faire de résolution vers un autre serveur étant donné qu'il possède le fichier de zone pour la zone en question. Il s'agit du fichier de zone db.30.98.160.in-addr.zone. Il répondra directement avec le contenu de ce fichier soit l'entrée suivante :

170 IN PTR ourpc.lte07.ch.

**P13:** Dessiner le diagramme en flèches des échanges observés.

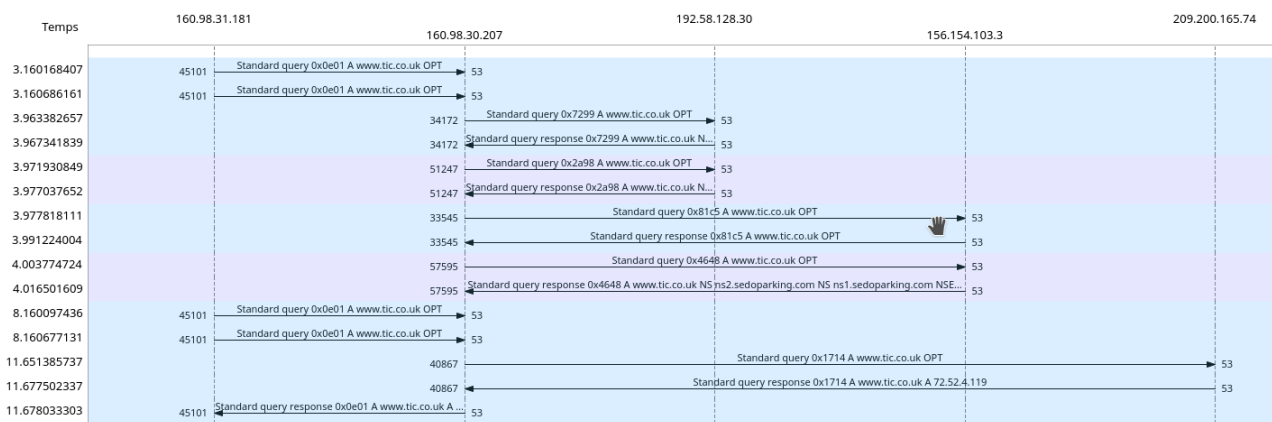


Figure 9 – Graphe des flux lord de la résolution DNS de www.tic.ac.uk

**P14:** Combien de requêtes effecture votre serveur DNS pour résoudre la requête ci-dessus?

On peut observer que le serveur effectue 4 requête sur 2 serveurs différents

## 4 Conclusion

Josué Tille

Marc Roten