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

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 à la réponse à notre question qui est ‘‘160.98.31.170’’.

P2: Décrivez les différents paramètres de configurstions 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 tlabs.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 pourons 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 exclaves. Il y aura notament : 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 chaques 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 authorité pour la zone en question. On a donc ici notre serveur DNS `ourpc.lte07.ch.` et aussi le serveur `tlabs.tic.eia-fr.ch.` qui a aussi authorité 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 toujour 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 lieux 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 authorité sur la zone.

NS Il est obligatoir 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 cherchan 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 resolveur DNS de connaitre l'adresse IP des serveurs Racines. Etant 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 obligatoir 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 – Catpure 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 enregistrées ? Commentez !

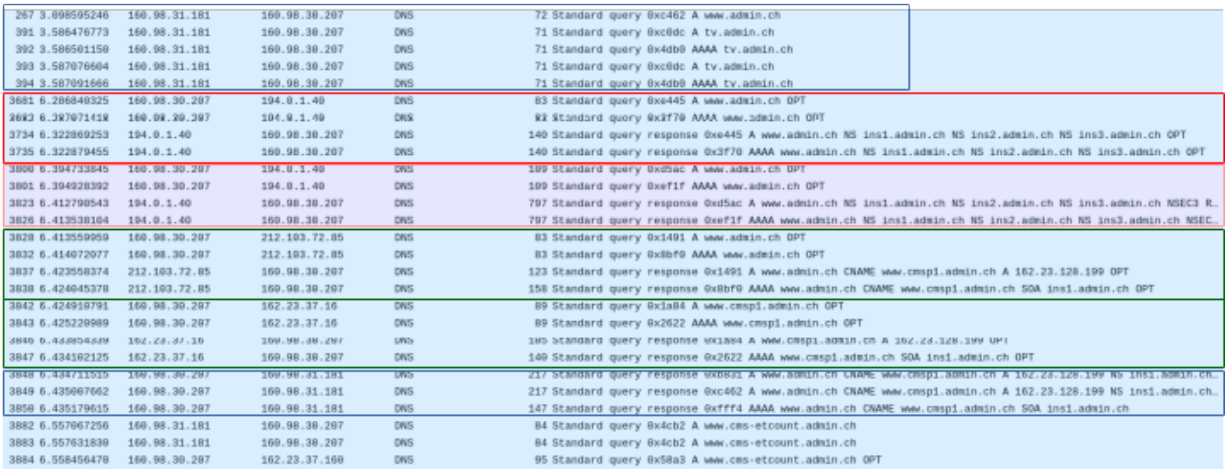

Figure 5 – Catpure de toutes les requetes effectuée lors de la consulation de la page ''www.admin.ch'' - En Bleu : Requetes PC <-> Résolveur DNS, En rose : Requetes Résolveur DNS <-> serveur authoritaire pour .ch, En Vert : Résolveur DNS <-> Serveur authoritaire pour admin.ch

On peut remarquer que au début le notre PC enverra une requête au serveur DNS pour connaitre l'adresse ip pour le domaine www.admin.ch. Ensuite le serveur effecturera 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 requete 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 requete aux serveur serveur authoritaire de admin.ch (ip 212.193.72.85, 162.23.37.16).

Nous avons constaté que dans ces requetes nous avons pas de communication avec les root serveur. Cela est probablement du au fait que l'adresse des serveur authoritaire pour .ch était déjà dans le cache de notre résolveur (malgèrs 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 requetes et les reponses. Nous avons aussi observé l'utilisations de 2 protocoles de transport soit UDP et TCP pour le DNS.

Figure 6 – Observation 2 requetes 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 !

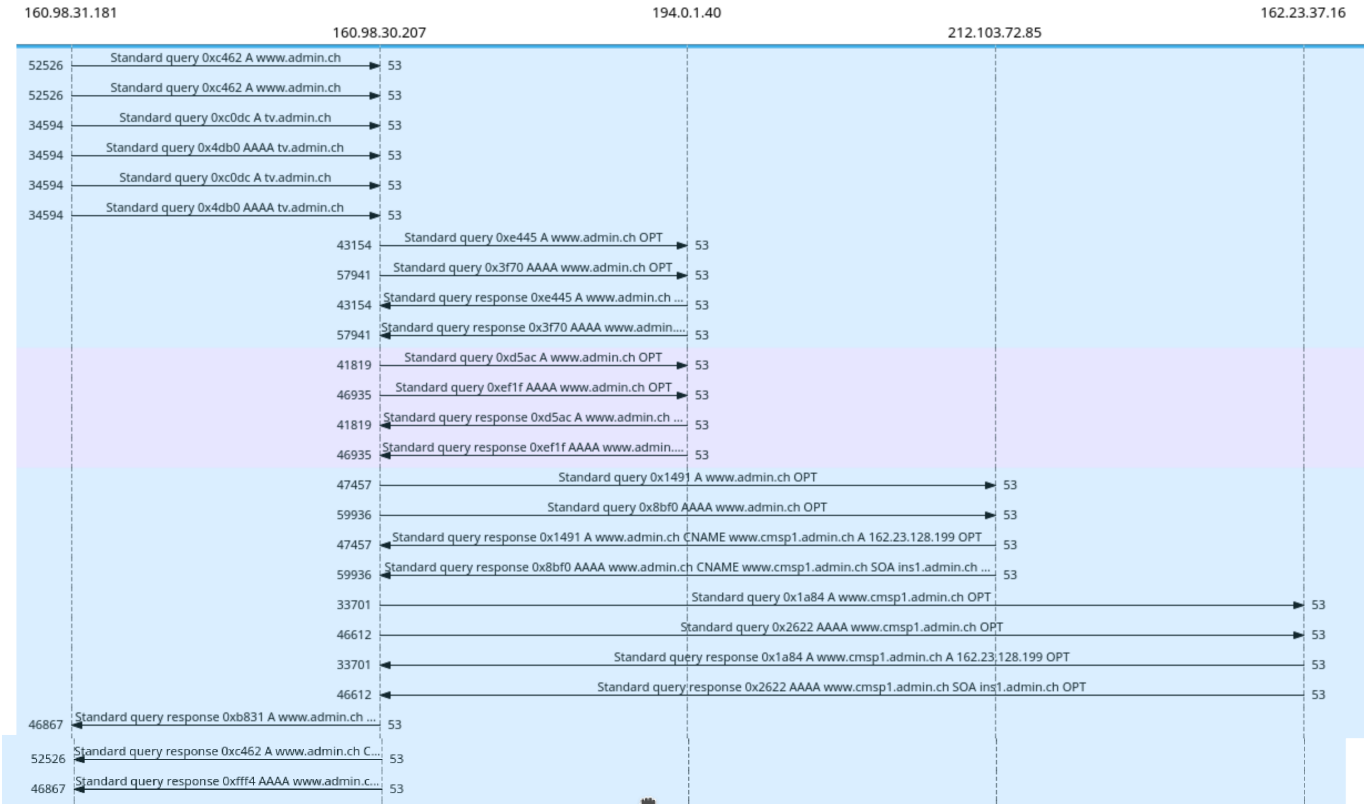

Figure 7 – Digramme en flèches de la requête DNS www.admin.ch depuis notre notebook.

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 requete DNS inverse. Les types de message serons très semblables aux précédentes : Une requete 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 lieux d'un enregistrement A.

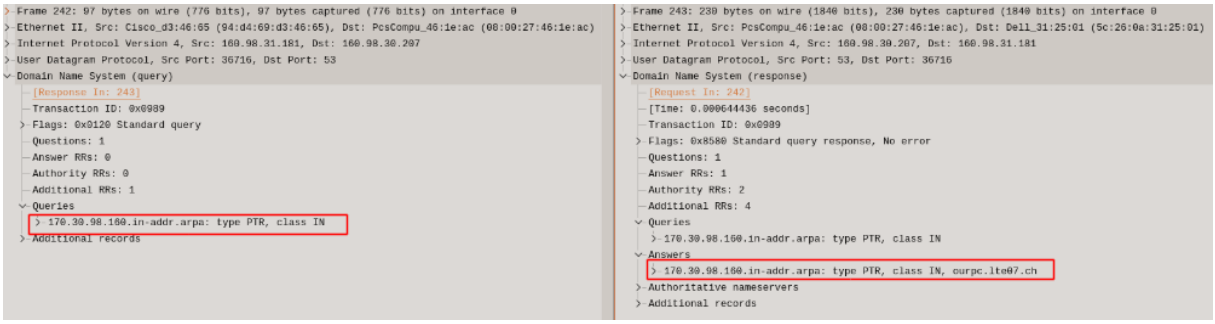

Figure 8 – Vue détaillé de la requête et de la réponse

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.

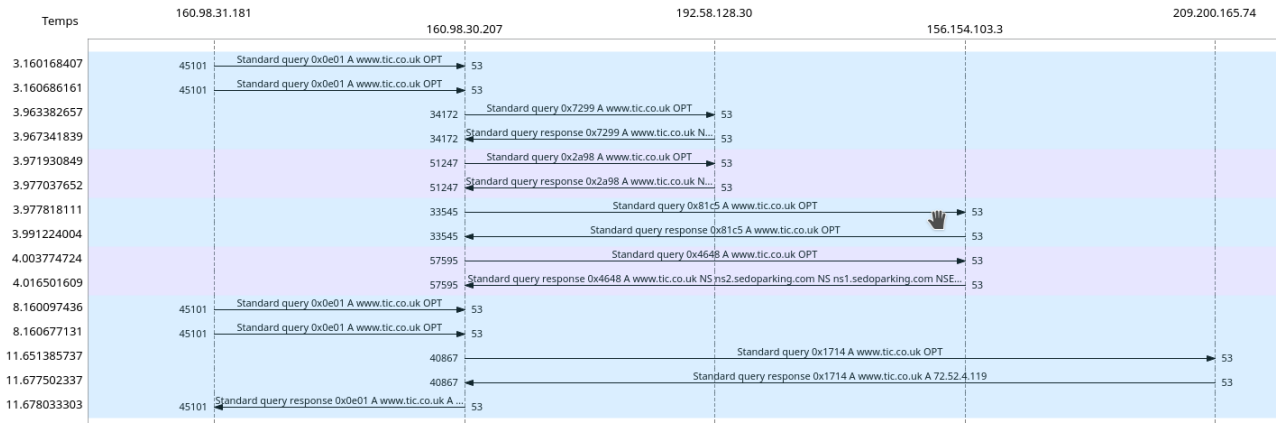

Figure 9 – Graphe des flux lord de la résolution DNS de www.tic.ac.uk

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

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

4 Conclusion

Josué Tille Marc Roten