

Exercice Pratiques de DNS

Ilyas Bambrik

Table des matières



I - DNS	3
1. Travail demandé	3
2. Exercice : Commandes DNS	3

DNS

I

1. Travail demandé

Pour chaque capture d'écran existante dans cette fiche TP, vous devez avoir la même capture afin de répondre aux questions lors de la consultation.

2. Exercice : Commandes DNS

Ouvrez votre invité de commande et tapez `ipconfig /all` (ifconfig pour linux) et ensuite repérez votre configuration DNS pour l'interface avec la quelle vous êtes connecté sur Internet. Vous pouvez voir l'adresse IP de votre serveur DNS (voir la figure en bas)

```

Windows PowerShell
Carte réseau sans fil Connexion au réseau local* 3 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Adresse physique . . . . . : 4A-51-B7-D4-C7-1D
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui

Carte réseau sans fil Wi-Fi :

Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : Intel(R) Dual Band Wireless-AC 7260
Adresse physique . . . . . : 48-51-B7-D4-C7-1D
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
Adresse IPv6. . . . . : fd00:664b:6dc1:aa00:b152:4f6a:ae26:9875(préfééré)
Adresse IPv6 temporaire . . . . . : fd00:664b:6dc1:aa00:f520:ce2c:5415:d0b1(préfééré)
Adresse IPv6 de liaison locale. . . . . : fe80::b152:4f6a:ae26:9875%18(préfééré)
Adresse IPv4. . . . . : 192.168.1.6(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mercredi 12 décembre 2018 18:16:01
Bail expirant. . . . . : vendredi 14 décembre 2018 16:51:13
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 105402807
DUID de client DHCPv6. . . . . : 00-01-00-01-23-18-30-F1-B8-6B-23-9A-92-8E
Serveurs DNS. . . . . : 192.168.1.1

```

- Tapez `nslookup` (outil de résolution de nom de domaine) et ouvrez `wireshark` (ainsi que votre interface correspondante).
- Écrivez le nom de domaine suivant `tcpipguide.com` dans l'invité de commande `nslookup` ;
- Appliquez le filtre suivant dans Wireshark : `dns.qry.name == "tcpipguide.com"`
- L'envoi de la requête DNS retourne l'adresse IP du nom de domaine "`tcpipguide.com`". La requête transmise par le Resolver (client `nslookup`) est une demande d'enregistrement A (A == Adresse record) [voir la capture d'écran Wireshark]. Ce type d'enregistrement fait la correspondance entre un nom de domaine et l'adresse IP correspondante (voir le cours).
- Par la suite la réponse correspondante à la requête est l'enregistrement de type A contenant l'adresse IP de "`tcpipguide.com`".

```

> Windows PowerShell
PS C:\Users\DVSR> nslookup
Serveur par défaut : UnKnown
Address: 192.168.1.1

> tcpipguide.com
Serveur : UnKnown
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : tcpipguide.com
Address: 216.92.67.219
    
```

dns.qry.name=="tcpipguide.com"

No.	Tim	Source	Destination	Protocol	Length	Info
...	...	192.168.1.6	192.168.1.1	DNS	74	Standard query 0x0002 A tcpipguide.com
...	...	192.168.1.1	192.168.1.6	DNS	90	Standard query response 0x0002 A tcpipguide.com A 216.92.67.219

> Frame 37: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 > Ethernet II, Src: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d), Dst: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa)
 > Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 54004, Dst Port: 53
 > Domain Name System (query)
 [Response In: 38]
 Transaction ID: 0x0002
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > tcpipguide.com: type A, class IN

dns.qry.name=="tcpipguide.com"

No.	Tim	Source	Destination	Protocol	Length	Info
...	...	192.168.1.6	192.168.1.1	DNS	74	Standard query 0x0002 A tcpipguide.com
...	...	192.168.1.1	192.168.1.6	DNS	90	Standard query response 0x0002 A tcpipguide.com A 216.92.67.219

> Frame 38: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
 > Ethernet II, Src: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa), Dst: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
 > User Datagram Protocol, Src Port: 53, Dst Port: 54004
 > Domain Name System (response)
 [Request In: 37]
 [Time: 0.001530000 seconds]
 Transaction ID: 0x0002
 > Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > tcpipguide.com: type A, class IN
 > Answers
 > tcpipguide.com: type A, class IN, addr 216.92.67.219

- Pour récupérer l'adresse IPv6 d'un nom de domaine (si ce domaine possède une adresse IPv6 public), tapez dans l'invité de nslookup les commandes suivantes :

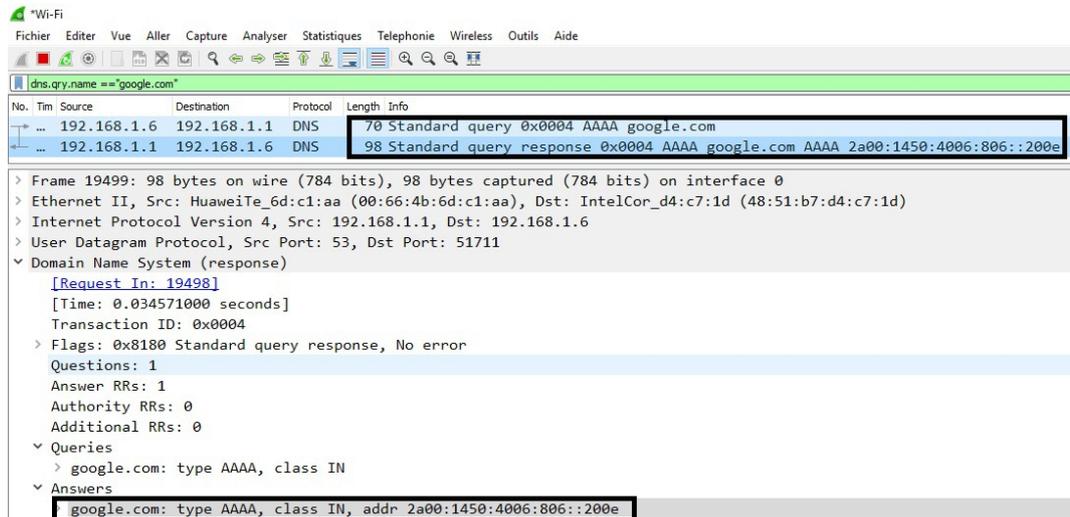
set type=AAAA

google.com

- Les deux commandes prétendantes permettent d'avoir l'adresse IPv6 public de google.com. *set type=AAAA* change le type d'enregistrement demandé par la requête DNS.

```
> set type=AAAA
> google.com
Serveur : UnKnown
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : google.com
Address: 2a00:1450:4006:806::200e
```



- Pour récupérer l'enregistrement CNAME (alias d'un nom de domaine) d'un nom de domaine (si ce domaine possède un alias), tapez dans l'invité de nslookup les commandes suivantes :

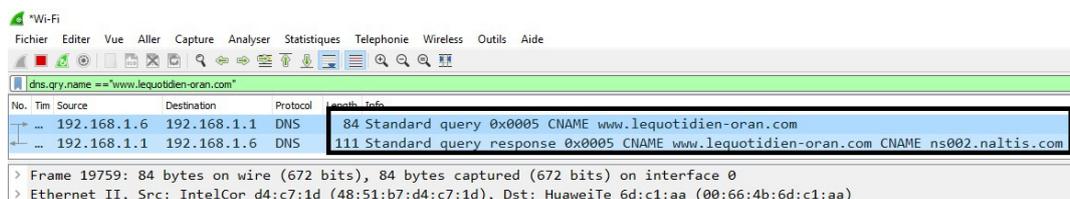
```
set type=CNAME
```

```
www.lequotidien-oran.com
```

- Les deux commandes prétendantes permettent d'avoir l'alias de *www.lequotidien-oran.com*. Dans cette exemple *www.lequotidien-oran.com* pointe sur *ns002.naltis.com* (voir la capture d'écran de).
- *ns002.naltis.com* possède l'adresse IP 91.121.146.205
- CNAME == *Canonical Name* ou bien nom canonique.
- Si vous procédez à exécuter un *ping* vers *www.lequotidien-oran.com* et *ns002.naltis.com*, vous remarquerais que les deux machines auront la même adresse IP (voir le déroulement du ping, l'adresse IP des deux domaines est identique).

```
> set type=CNAME
> www.lequotidien-oran.com
Serveur : UnKnown
Address: 192.168.1.1

Réponse ne faisant pas autorité :
www.lequotidien-oran.com canonical name = ns002.naltis.com
>
```



```

C:\Users\DVSR>ping www.lequotidien-oran.com

Envoi d'une requête 'ping' sur ns002.naltis.com [91.121.146.205] avec 32 octets de données :
Réponse de 91.121.146.205 : octets=32 temps=133 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=75 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=73 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=83 ms TTL=48

Statistiques Ping pour 91.121.146.205:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 73ms, Maximum = 133ms, Moyenne = 91ms

C:\Users\DVSR>ping ns002.naltis.com

Envoi d'une requête 'ping' sur ns002.naltis.com [91.121.146.205] avec 32 octets de données :
Réponse de 91.121.146.205 : octets=32 temps=74 ms TTL=48

Statistiques Ping pour 91.121.146.205:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 74ms, Maximum = 74ms, Moyenne = 74ms

C:\Users\DVSR>
    
```

- Pour récupérer les noms des serveurs mail dans un domaine, il suffit de changer le type de l'enregistrement demandé (set type=MX) :

set type=MX

google.com

- Les noms des serveurs retournés sont des noms de serveurs mail. La valeur de préférence permet de choisir entre plusieurs serveurs mail (une valeur de préférence plus petite indique une préférence supérieur par rapport aux autres serveurs mail disponibles) ; Dans cet exemple : Le serveur mail préféré de google est == *aspmx.l.google.com* (la valeur de préférence minimale);
- Plusieurs serveurs mail peuvent coexister dans un domaine pour que le système soit tolérant au pannes (s un serveur ne peut pas recevoir le mail entrant, le prochain mail selon la valeur de préférence est choisi pour l'échange du mail en question) ;
- *MX= Mail eXchanger* ;

```

Windows PowerShell
PS C:\Users\DVSR> nslookup
Serveur par défaut : UnKnown
Address: 192.168.1.1

> set type=mx
> google.com
Serveur : UnKnown
Address: 192.168.1.1

Réponse ne faisant pas autorité :
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
>
    
```