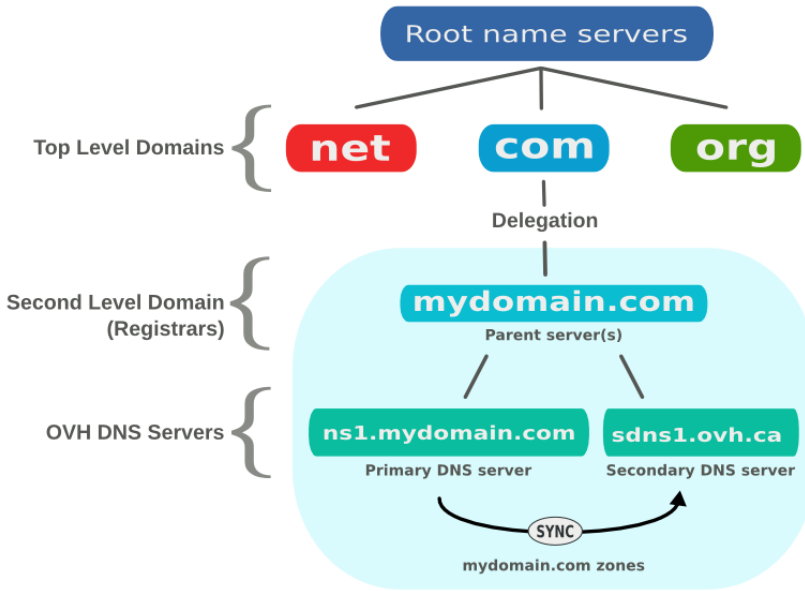

# - TP 1 -
# Services réseaux avancés – DNS

*par Édouard Lumet*



# Sommaire

# 1. Serveur DNS

## *1.1. Résolution standard*

1. Le fichier */etc/bind/named.conf* est l'endroit où sont renseignées les différentes zones DNS à raison d'une zone par domaine.

```
zone "domaineEL.rt" {   #déclaration d'une zone pour un NDD domaineel.rt. Rmq : la casse n'importe pas
        type master;    #le serveur est configuré en tant que maître pour ce domaine
        file "/etc/bind/db.domaineEL.rt"; #on précise ensuite le fichier qui contient les enregistrements
};
```

Le fichier */etc/bind/db.domaineEL.rt* pour notre configuration est le suivant :

```
$TTL 604800     #durée de vie de la ressource en cache
@ IN SOA machine root.domaineEL.rt. (  #déclaration de l'authorité, le serveur primaire de
                                       #root.domaineEL.rt est machine
        1 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS machine.domaineEL.rt. ;        #nom du serveur de nom

machine IN A 192.168.0.25       #enregistrement A indiquant l'@IP associée au NDD + sous-domaine
                                machine (machine.domaineel.rt)
smtp CNAME machine              #enregistrement CNAME alias du NDD précédent (smtp.domaineel.rt)
```

Ensuite, il existe deux commandes pour tester les configurations : *named-checkconf* pour tester */etc/bind/named.conf* et *named-checkzone* pour tester */etc/bind/db.domaineel.rt*. Une erreur a été détectée dans le second fichier : le nom de la machine que j'avais oublié de modifier par rapport à l'exemple ligne 2. *serveur* n'avait effectivement pas d'enregistrement A.

2. Tests : ping, nslookup et dig

Lors d'un ping vers *machine.domaineel.rt*, on peut voir que c'est bien l'adresse 192.168.0.25 qui est testée et qui répond. Cela veut dire que, à priori, le PC a réussi à résoudre en interrogeant son DNS (BIND) le NDD. Ceci est confirmé par un *nslookup* puis un *dig* montrant l'enregistrement DNS A fournit par l'autorité machine.domaineel.rt qui est notre serveur de nom récemment installé.

*Voir illustration ci-dessous*

```
iutrt2A@PC-25 ~ $ ping machine.domaineel.rt
PING machine.domaineel.rt (192.168.0.25) 56(84) bytes of data.
64 bytes from PC-25 (192.168.0.25): icmp_req=1 ttl=64 time=0.047 ms
64 bytes from PC-25 (192.168.0.25): icmp_req=2 ttl=64 time=0.029 ms
64 bytes from PC-25 (192.168.0.25): icmp_req=3 ttl=64 time=0.034 ms
64 bytes from PC-25 (192.168.0.25): icmp_req=4 ttl=64 time=0.031 ms
^C
--- machine.domaineel.rt ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.029/0.035/0.047/0.008 ms
iutrt2A@PC-25 ~ $ dig machine.domaineel.rt

; <<>> DiG 9.8.1-P1 <<>> machine.domaineel.rt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51670
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;machine.domaineel.rt.          IN      A

;; ANSWER SECTION:
machine.domaineel.rt.   604800  IN      A       192.168.0.25

;; AUTHORITY SECTION:
domaineel.rt.           604800  IN      NS      machine.domaineel.rt.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep  5 14:58:11 2016
;; MSG SIZE  rcvd: 68

iutrt2A@PC-25 ~ $ nslookup machine.domaineel.rt
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   machine.domaineel.rt
Address: 192.168.0.25

iutrt2A@PC-25 ~ $
```

*Test des commandes ping, nslookup et dig auprès du NDD machine.domaineel.rt*

## 1.2. Résolution inverse

La résolution inverse consiste à trouver l'adresse IP à partir du NDD.

On déclare donc une nouvelle zone dans le fichier */etc/bind/named.conf* :

```
zone "0.168.192.in-addr.arpa" {  #on déclare une zone inverse avec les trois premiers
                                 #octets de l'@IP (classe C)
        type master;     #pour cette zone également le serveur est maître
        file "/etc/bind/db.192";  #les enregistrements sont contenus dans le fichier
                                 #/etc/bind/db.192
};
```

Les enregistrements de la zone inverse sont les suivants :

```
$TTL    604800
@       IN      SOA     machine.domaineEL.rt root.domaineEL.rt (      #l'autorité est la même que pour
                                                                      #la zone 'normale'
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200                 ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      machine.domaineEL.rt.          #de même pour le serveur de nom
                                                       #qui est machine.domaineel.rt
25      IN      PTR     machine.domaineEL.rt. #l'enregistrement PTR permet de pointer l'@IP 192.168.0.25
                                              #vers le NDD machine.domaineel.rt
```

Un dig ou host sur 192.168.0.25 nous indique bien en retour le nom de domaine que l'on a configuré.

```
iutrt2A@PC-25 ~ $ dig -x 192.168.0.25

; <<>> DiG 9.8.1-P1 <<>> -x 192.168.0.25
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25189
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;25.0.168.192.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
25.0.168.192.in-addr.arpa. 604800 IN    PTR     machine.domaineEL.rt.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa. 604800  IN      NS      machine.domaineEL.rt.

;; ADDITIONAL SECTION:
machine.domaineEL.rt.   604800  IN      A       192.168.0.25

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep  5 15:27:02 2016
;; MSG SIZE  rcvd: 107

iutrt2A@PC-25 ~ $ host 192.168.0.25
25.0.168.192.in-addr.arpa domain name pointer machine.domaineEL.rt.
```

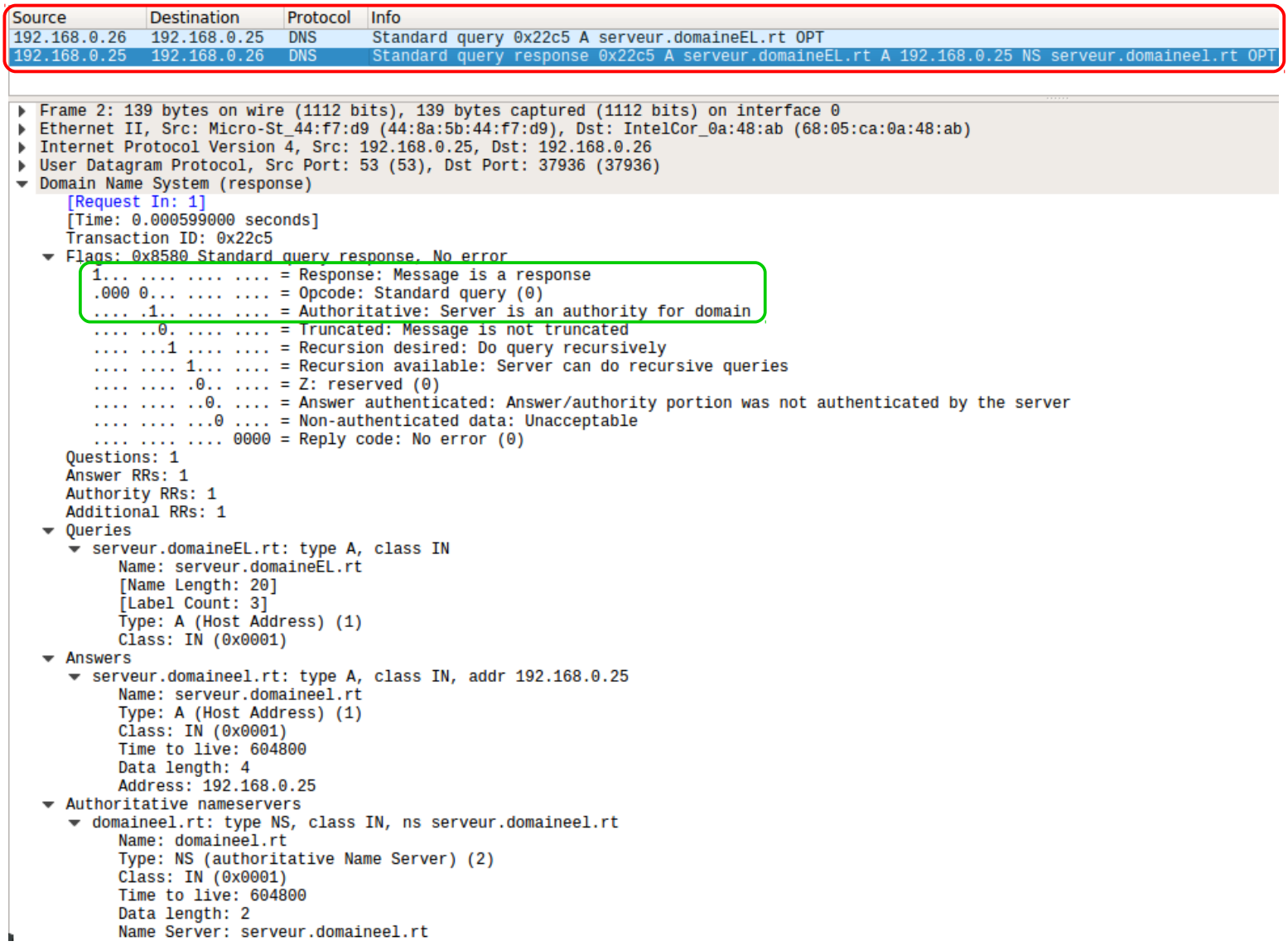
## 2. Client DNS

Disposant d'un serveur DNS prêt et configuré, on peut effectuer un test avec un autre poste en l'indiquant comme serveur de noms sur ce dernier client.

Nous avons crée un binôme entre PC-25 (192.168.0.25) et PC-26 (192.168.0.26). Le premier est le serveur, le second est le client.

Sur PC-26 on ajoute cette ligne au fichier */etc/resolv.conf* : **nameserver 192.168.0.25**

Lorsque l'on exécute la commande **dig serveur.domaineel.rt** depuis le client, on observe alors les échanges suivants :



| Source | Destination | Protocol | Info |
|---|---|---|---|
| 192.168.0.26 | 192.168.0.25 | DNS | Standard query 0x22c5 A serveur.domaineEL.rt OPT |
| 192.168.0.25 | 192.168.0.26 | DNS | Standard query response 0x22c5 A serveur.domaineEL.rt A 192.168.0.25 NS serveur.domaineel.rt OPT |

```
▸ Frame 2: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
▸ Ethernet II, Src: Micro-St_44:f7:d9 (44:8a:5b:44:f7:d9), Dst: IntelCor_0a:48:ab (68:05:ca:0a:48:ab)
▸ Internet Protocol Version 4, Src: 192.168.0.25, Dst: 192.168.0.26
▸ User Datagram Protocol, Src Port: 53 (53), Dst Port: 37936 (37936)
▾ Domain Name System (response)
    [Request In: 1]
    [Time: 0.000599000 seconds]
    Transaction ID: 0x22c5
  ▾ Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▾ serveur.domaineEL.rt: type A, class IN
        Name: serveur.domaineEL.rt
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ serveur.domaineel.rt: type A, class IN, addr 192.168.0.25
        Name: serveur.domaineel.rt
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 604800
        Data length: 4
        Address: 192.168.0.25
  ▾ Authoritative nameservers
    ▾ domaineel.rt: type NS, class IN, ns serveur.domaineel.rt
        Name: domaineel.rt
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 604800
        Data length: 2
        Name Server: serveur.domaineel.rt
```

On voit une première trame qui correspond à la requête DNS de type A pour *serveur.domaineel.rt* et une seconde trame correspondant à la réponse du serveur et indiquant l'adresse IPv4 correspondant au NDD.

Dans le détail de la réponse (vert), on identifie les flags étudiée en cours et en TD. Le premier (RCODE) est à 1 car c'est un message de réponse. Le deuxième (OPCODE) est à 0 car il s'agit d'une résolution de nom et non d'une résolution inverse. Le troisième (AA) est à 1 car le serveur interrogé fait autorité sur la zone *domaineel.rt*.

# 3. Ajouts

## 3.1. Serveur secondaire

Dans le fichier */etc/bind/named.conf* sur le serveur primaire (ici PC-25, PC-26 sera le serveur secondaire), on ajoute dans chaque zone la ligne :

**allow-transfer { 192.168.0.26 ; } ;**

Dans ce même fichier, sur le serveur secondaire, on indique dans chaque zone non plus **type master ;** mais **type slave ;**

Ensuite pour **file** on indique le fichier */var/cache/bind/db.domaineel.rt* afin que le serveur secondaire puisse écrire les infos de la zone db.domaineel.rt qu'il va recevoir du serveur primaire.

Enfin, on indique l'adresse du serveur primaire en ajoutant cette ligne :

**masters { 192.168.0.25 } ;**

À l'aide de Wireshark, on observe l'échange entre les deux serveurs lors de la récupération des informations de zone :

| Source | Destination | Protocol | Info |
|---|---|---|---|
| 192.168.0.26 | 192.168.0.25 | DNS | Standard query 0x22c5 A serveur.domaineEL.rt OPT |
| 192.168.0.25 | 192.168.0.26 | DNS | Standard query response 0x22c5 A serveur.domaineEL.rt A 192.168.0.25 NS serveur.domaineel.rt OPT |

```
▸ Frame 2: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
▸ Ethernet II, Src: Micro-St_44:f7:d9 (44:8a:5b:44:f7:d9), Dst: IntelCor_0a:48:ab (68:05:ca:0a:48:ab)
▸ Internet Protocol Version 4, Src: 192.168.0.25, Dst: 192.168.0.26
▸ User Datagram Protocol, Src Port: 53 (53), Dst Port: 37936 (37936)
▾ Domain Name System (response)
    [Request In: 1]
    [Time: 0.000599000 seconds]
    Transaction ID: 0x22c5
  ▾ Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▾ serveur.domaineEL.rt: type A, class IN
        Name: serveur.domaineEL.rt
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ serveur.domaineel.rt: type A, class IN, addr 192.168.0.25
        Name: serveur.domaineel.rt
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 604800
        Data length: 4
        Address: 192.168.0.25
  ▾ Authoritative nameservers
    ▾ domaineel.rt: type NS, class IN, ns serveur.domaineel.rt
        Name: domaineel.rt
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 604800
        Data length: 2
        Name Server: serveur.domaineel.rt
```