

Wang Pengchao G1 TDA
Mohamed Amine Mzoughi G1 TDA

TP 1 - Domain Name Service (DNS)

EXERCICE 1 -Commandes de base

1- A l'aide de la commande host, déterminez l'IP de lipn.fr, et celle du serveur de mail de ce domaine

1)

On utilise la commande host pour savoir l'adresse IP de lipn.fr qui est : 194.254.163.36

On a aussi l'adresse du mail qui est : 10 mail.lipn.fr

```
azer@q20303:~$ host lipn.fr
lipn.fr has address 194.254.163.36
lipn.fr mail is handled by 10 mail.lipn.fr.
azer@q20303:~$ █
```

2- Avec host -v, indiquez le serveur DNS autoritaire sur lipn.fr. A quel entreprise appartient-il ?

2) On a utilisé la commande host -v lipn.fr , on retrouve 3 serveurs autoritaires sur lipn.fr qui sont : 1- b.dns.gandi.net

- 2- a.dns.gandi.net
- 3- c.dns.gandi.net

Ils appartiennent à l'entreprise gandi.

```
;; AUTHORITY SECTION:  
lipn.fr.          8455    IN      SOA     a.dns.gandi.net. hostmaster.gandi.net. 1468472083 10800 3600 604800 10800  
Received 87 bytes from 192.168.1.20#53 in 2 ms  
Trying "lipn.fr"  
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 27716  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4  
;; QUESTION SECTION:  
;lipn.fr.          IN      MX  
;; ANSWER SECTION:  
lipn.fr.          16587   IN      MX      10 mail.lipn.fr.  
;; AUTHORITY SECTION:  
lipn.fr.          5605    IN      NS      b.dns.gandi.net.  
lipn.fr.          5605    IN      NS      a.dns.gandi.net.  
lipn.fr.          5605    IN      NS      c.dns.gandi.net.
```

3- Retrouver l'adresse IP de lipn.fr à l'aide de la commande dig (cette commande est plus complète que host, voir par exemple

<https://mediatemple.net/community/products/dv/2044-4130/understanding-the-dig-command>).

3)

On a utilisé la commande dig lipn.fr , on remarqu'il y a plus d'information que la commande "host".

On aperçoit l'adresse IP : 192.254.163.36

```
azer@q20303:~$ dig lipn.fr
; <>> DiG 9.10.3-P4-Debian <>> lipn.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61329
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;
;; QUESTION SECTION:
;lipn.fr.                      IN      A
;
;; ANSWER SECTION:
lipn.fr.          7885    IN      A      194.254.163.36
;
;; Query time: 0 msec
;; SERVER: 192.168.1.20#53(192.168.1.20)
;; WHEN: Thu Sep 08 14:23:27 CEST 2022
;; MSG SIZE  rcvd: 41
azer@q20303:~$
```

4- Même question avec nslookup

4)

On a utilisé la commande nslookup lipn.fr , on remarqu'il y a l'adresse IP du serveur : 192.168.1.20 et celle de lipn.fr : 194.254.163.36

```
azer@q20303:~$ nslookup lipn.fr
Server:      192.168.1.20
Address:     192.168.1.20#53

Non-authoritative answer:
Name:   lipn.fr
Address: 194.254.163.36

azer@q20303:~$
```

EXERCICE 2 -Nommage statique

1- Consultez le fichier /etc/nsswitch.conf. Quelle ligne détermine l'ordre d'utilisation des méthodes de résolution ?

1)On a utilisé la commande nano /etc/nsswitch.conf.
la ligne qui détermine l'ordre d'utilisation des méthodes de résolution est la ligne hosts qui est soulignée.
On est dans la résolution statique "files"

```
| GNU nano 2.7.4                                     Fichier : /etc/nsswitch.conf
| # /etc/nsswitch.conf
| #
| # Example configuration of GNU Name Service Switch functionality.
| # If you have the `glibc-doc-reference` and `info` packages installed, try:
| # `info libc "Name Service Switch"' for information about this file.

passwd:      compat
group:       compat
shadow:      compat
gshadow:     files

hosts:      files myhostname mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

2- Quelles sont les adresses IP attribuées à vos machines ?
Qui(quel logiciel ou protocole) leur a attribué ? A quel moment ?

2)

L'adresse du première machine est : 192.168.43.3/24

L'adresse du deuxième machine est : 192.168.43.4/24

C'est le protocole DHCP qui leur a attribué.

Lorsque le client demande au serveur local (le traducteur) ,on envoie des requêtes au serveur DNS.

```
azer@q20303:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 78:45:c4:40:a1:13 brd ff:ff:ff:ff:ff:ff
        inet 192.168.43.3/24 brd 192.168.43.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::7a45:c4ff:fe40:a113/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:0a:f7:16:bc:e9 brd ff:ff:ff:ff:ff:ff
```

```
mzmz@q20304:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 78:45:c4:40:9f:05 brd ff:ff:ff:ff:ff:ff
        inet 192.168.43.4/24 brd 192.168.43.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::7a45:c4ff:fe40:9f05/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:0a:f7:16:c7:b8 brd ff:ff:ff:ff:ff:ff
```

3- Modifier les fichiers `/etc/hosts` pour attribuer des noms à vos machines. Notez ces noms dans votre compte-rendu. A l'aide de ping, vérifiez que les noms sont bien utilisés.

3)

l'adresse du serveur : 192.168.43.3/24

l'adresse du client : 192.168.43.4/24

```
GNU nano 2.7.4                                     Fichier : /etc/hosts

127.0.0.1      localhost
127.0.1.1      q20303.iutv.univ-paris13.fr      q20303

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.43.3 serveur
192.168.43.4 client
```

On a pu ping le client au serveur :

```
q20303: root /home/azer# ping serveur
PING serveur (192.168.43.4) 56(84) bytes of data.
64 bytes from serveur (192.168.43.4): icmp_seq=1 ttl=64 time=0.160 ms
64 bytes from serveur (192.168.43.4): icmp_seq=2 ttl=64 time=0.180 ms
64 bytes from serveur (192.168.43.4): icmp_seq=3 ttl=64 time=0.143 ms
64 bytes from serveur (192.168.43.4): icmp_seq=4 ttl=64 time=0.173 ms
64 bytes from serveur (192.168.43.4): icmp_seq=5 ttl=64 time=0.175 ms
^C
--- serveur ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.143/0.166/0.180/0.015 ms
q20303: root /home/azer#
```

On a pu ping du serveur au client :

```
q20304: root /home/mzmz# ping client
PING client (192.168.43.3) 56(84) bytes of data.
64 bytes from client (192.168.43.3): icmp_seq=1 ttl=64 time=0.143 ms
64 bytes from client (192.168.43.3): icmp_seq=2 ttl=64 time=0.171 ms
64 bytes from client (192.168.43.3): icmp_seq=3 ttl=64 time=0.171 ms
64 bytes from client (192.168.43.3): icmp_seq=4 ttl=64 time=0.171 ms
64 bytes from client (192.168.43.3): icmp_seq=5 ttl=64 time=0.172 ms
64 bytes from client (192.168.43.3): icmp_seq=6 ttl=64 time=0.171 ms
^C
--- client ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5125ms
rtt min/avg/max/mdev = 0.143/0.166/0.172/0.016 ms
```

4- Quelle est l'adresse IP du serveur DNS utilisée par vos machines? Dans quel fichier de configuration figure-t-elle ? A quel moment et par qui a été attribuée à cette adresse ?

4)

On utilise eth1 pour pouvoir créer un réseau local entre les deux machines.

```
GNU nano 2.7.4                                     Fichier : /etc/hosts

127.0.0.1      localhost
127.0.1.1      q20303.iutv.univ-paris13.fr      q20303

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.150.10.1 serveur
192.150.10.2 client
```

L'adresse IP du serveur DNS utilisée par les machines est

```
GNU nano 2.7.4                                     Fichier : /etc/resolv.conf

domain iutv.univ-paris13.fr
search iutv.univ-paris13.fr
nameserver 192.168.1.20
nameserver 192.168.1.73
```

Il se trouve dans le fichier /etc/resolv.conf.

Il est attribué par le DHCP

EXERCICE 3 -Serveur DNS bind9

1- Installer le paquetage bind9 . Quels sont les paquetages automatiquement installées avec lui (ses dépendances) ?

```
q20303: root /home/azer# apt-get update
Ign:1 http://ftp.fr.debian.org/debian stretch InRelease
Récception de:2 http://security.debian.org stretch/updates InRelease [59,1 kB]
Récception de:3 http://ftp.fr.debian.org/debian stretch-updates InRelease [93,6 kB]
Récception de:4 http://download.virtualbox.org/virtualbox/debian stretch InRelease [7 782 B]
Récception de:5 http://ftp.fr.debian.org/debian stretch Release [118 kB]
Récception de:6 http://ftp.fr.debian.org/debian stretch Release.gpg [3 177 B]
Récception de:7 http://security.debian.org stretch/updates/main Sources [413 kB]
Récception de:8 http://security.debian.org stretch/updates/non-free Sources [3 568 B]
Récception de:9 http://security.debian.org stretch/updates/main amd64 Packages [782 kB]
Récception de:10 http://security.debian.org stretch/updates/main Translation-en [368 kB]
Récception de:11 http://security.debian.org stretch/updates/contrib amd64 Packages [1 760 B]
Récception de:12 http://security.debian.org stretch/updates/non-free amd64 Packages [14,1 kB]
Récception de:13 http://security.debian.org stretch/updates/non-free Translation-en [21,3 kB]
Récception de:14 http://download.virtualbox.org/virtualbox/debian stretch/contrib amd64 Packages [2 247 B]
Récception de:15 http://ftp.fr.debian.org/debian stretch/main Sources [6 736 kB]
Récception de:16 http://ftp.fr.debian.org/debian stretch/non-free Sources [79,1 kB]
Récception de:17 http://ftp.fr.debian.org/debian stretch/contrib Sources [44,5 kB]
Récception de:18 http://ftp.fr.debian.org/debian stretch/main amd64 Packages [7 080 kB]
Récception de:19 http://ftp.fr.debian.org/debian stretch/main Translation-en [5 377 kB]
Récception de:20 http://ftp.fr.debian.org/debian stretch/contrib amd64 Packages [50,7 kB]
Récception de:21 http://ftp.fr.debian.org/debian stretch/contrib Translation-en [45,8 kB]
Récception de:22 http://ftp.fr.debian.org/debian stretch/non-free amd64 Packages [78,3 kB]
Récception de:23 http://ftp.fr.debian.org/debian stretch/non-free Translation-en [80,2 kB]
21,5 Mo réceptionnés en 4s (5 019 ko/s)
Lecture des listes de paquets... Fait
```

```
q20303: root /home/azer# apt-get install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
 libdirectfb-1.2-9 libgles1-mesa libiso9660-8 libonig2 libqdbm14 libvcdinfo0 libvlccore8
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
The following additional packages will be installed:
 bind9-host bind9utils dnsutils libbind9-140 libdns162 libirs141 libisc160 libisccc140 libisccfg140 lib
Paquets suggérés :
 bind9-doc resolvconf ufw rblcheck
Les NOUVEAUX paquets suivants seront installés :
 bind9 bind9utils libirs141
Les paquets suivants seront mis à jour :
 bind9-host dnsutils libbind9-140 libdns162 libisc160 libisccc140 libisccfg140 liblwres141
8 mis à jour, 3 nouvellement installés, 0 à enlever et 392 non mis à jour.
Il est nécessaire de prendre 3 960 ko dans les archives.
Après cette opération, 3 403 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] o
Récception de:1 http://security.debian.org stretch/updates/main amd64 bind9-host amd64 1:9.10.3.dfsg.P4-1
Récception de:2 http://security.debian.org stretch/updates/main amd64 dnsutils amd64 1:9.10.3.dfsg.P4-12
Récception de:3 http://security.debian.org stretch/updates/main amd64 libisc160 amd64 1:9.10.3.dfsg.P4-12
Récception de:4 http://security.debian.org stretch/updates/main amd64 libdns162 amd64 1:9.10.3.dfsg.P4-12
```

Voici les paquetages automatiquement installées avec lui.

```
q20303: root /home/azer# apt-cache depends bind9
bind9
  Dépend: libbind9-140
  Dépend: libc6
  Dépend: libcap2
  Dépend: libcomerr2
  Dépend: libdns162
  Dépend: libgeoip1
  Dépend: libgssapi-krb5-2
  Dépend: libirs141
  Dépend: libisc160
  Dépend: libisccc140
  Dépend: libisccfg140
  Dépend: libk5crypto3
  Dépend: libkrb5-3
  Dépend: liblwres141
  Dépend: libssl1.0.2
  Dépend: libxml2
  |Dépend: debconf
  |  Dépend: <debconf-2.0>
  |    cdebconf
  |    debconf
  Dépend: init-system-helpers
  Dépend: netbase
  Dépend: adduser
  Dépend: lsb-base
  Dépend: bind9utils
  Dépend: net-tools
  Est en conflit avec: apparmor-profiles
  Est en conflit avec: <bind>
  Suggère: dnsutils
    knot-dnsutils
  Suggère: bind9-doc
  Suggère: resolvconf
    openresolv
  Suggère: ufw
  Remplace: apparmor-profiles
  Remplace: <bind>
  Remplace: bind9utils
  Remplace: dnsutils
q20303: root /home/azer#
```

2- Créez un répertoire

/var/named/maitre

qui contiendra les définitions des fichiers de zone sur le serveur.

Quelle commande utilisez-vous ?

2)

On utilise la commande mkdir -p

```
q20303: root /var# mkdir -p /var/named/maitre  
q20303: root /var#
```

3- Le fichier de configuration principal de bind9 sous Linux Debian 9 est /etc/bind/named.conf. Il charge trois fichiers. Lesquels ?

```
GNU nano 2.7.4                                     Fichier : /etc/bind/named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

4- Modifier le fichier

/etc/bind/named.conf

```
GNU nano 2.7.4                                     Fichier : /etc/bind/named.conf

options {
    directory "/var/named" ;
    listen-on { any; };
    allow-query { any; };
} ;

zone equipe.p13.fr {
    type master ;
    file "maitre/equipe.p13.fr" ;
    allow-update { none ; };
    notify no ;
} ;
```

5- Vérifier la syntaxe du fichier de configuration avec named-checkconf : si tout est bon, la commande n'affiche rien.

```
q20303: root ~# named-checkconf  
q20303: root ~#
```

6- Créez le fichier de zone,
/var/named/maitre/equipe.p13.fr:

On crée avec la commande “touch”

```
q20303: root ~# touch /var/named/maitre/equipe.p13.fr  
q20303: root ~#
```

```
GNU nano 2.7.4                                     Fichier : /var/named/maitre/equipe.p13.fr

$TTL 180

@ IN      SOA     serveur.equipe.p13.fr.      root.serveur.equipe.p13.fr. (
    2017102601      ; Serial
    120            ; Refresh
    60             ; Retry
    300            ; Expire
    180            ; Minimum TTL
)

                IN      NS      serveur.equipe.p13.fr.
serveur      IN      TXT      "Domaine de equipe 1 "
client       IN      A        10.10.88.1
ns           IN      A        10.10.88.2
m1           CNAME   serveur
machine1    CNAME   serveur
m2           CNAME   client
machine2    CNAME   client
```

7- Vérifier la syntaxe du fichier de zone avec named-checkzone : quels arguments faut-il utiliser ?

```
q20303: root ~# named-checkzone equipe.p13.fr /var/named/maitre/equipe.p13.fr
zone equipe.p13.fr/IN: loaded serial 2017102601
OK
q20303: root ~#
```

8- Lancer le serveur :

```
/etc/init.d/bind9 restart
```

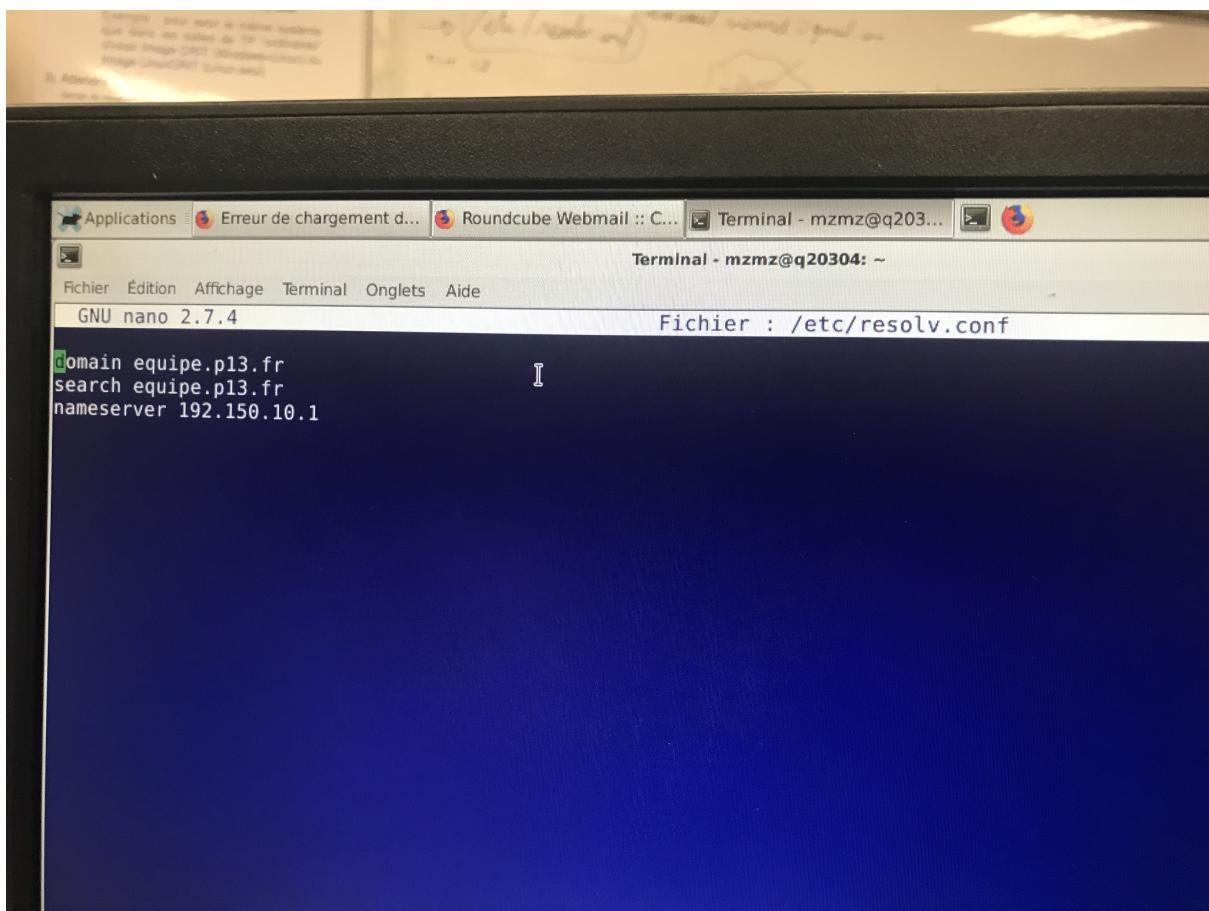
.Surveillez le log dans une autre fenêtre de terminal, avec tail -f /var/log/daemon.log

```
q20303: root ~# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
q20303: root ~#
```

```
azer@q20303:~$ tail -f /var/log/daemon.log
Sep 8 16:36:51 q20303 named[6493]: automatic empty zone: EMPTY.ARPA
Sep 8 16:36:51 q20303 named[6493]: configuring command channel from '/etc/bind/rndc.key'
Sep 8 16:36:51 q20303 named[6493]: command channel listening on 127.0.0.1#953
Sep 8 16:36:51 q20303 named[6493]: configuring command channel from '/etc/bind/rndc.key'
Sep 8 16:36:51 q20303 named[6493]: command channel listening on ::1#953
Sep 8 16:36:51 q20303 named[6493]: the working directory is not writable
Sep 8 16:36:51 q20303 named[6493]: managed-keys-zone: loaded serial 0
Sep 8 16:36:51 q20303 named[6493]: zone equipe.p13.fr/IN: loaded serial 2017102601
Sep 8 16:36:51 q20303 named[6493]: all zones loaded
Sep 8 16:36:51 q20303 named[6493]: running
Sep 8 16:39:00 q20303 dhclient[970]: DHCPREQUEST of 192.168.43.3 on eth0 to 192.168.43.254 port 67
Sep 8 16:39:00 q20303 dhclient[970]: DHCPCACK of 192.168.43.3 from 192.168.43.254
Sep 8 16:39:00 q20303 dhclient[970]: bound to 192.168.43.3 -- renewal in 136 seconds.
Sep 8 16:39:04 q20303 systemd[1]: Starting Clean php session files...
Sep 8 16:39:04 q20303 systemd[1]: Started Clean php session files.
Sep 8 16:39:15 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 5
Sep 8 16:39:20 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 7
Sep 8 16:39:27 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
Sep 8 16:39:35 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 15
Sep 8 16:39:51 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 16
Sep 8 16:40:07 q20303 dhclient[1426]: DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 9
Sep 8 16:40:16 q20303 dhclient[1426]: No DHCPOFFERS received.
Sep 8 16:40:16 q20303 dhclient[1426]: No working leases in persistent database - sleeping.
```

9- Configurer l'autre PC (client) afin qu'il utilise le DNS que vous venez de mettre en place (expliquez ce que vous devez faire pour cela).

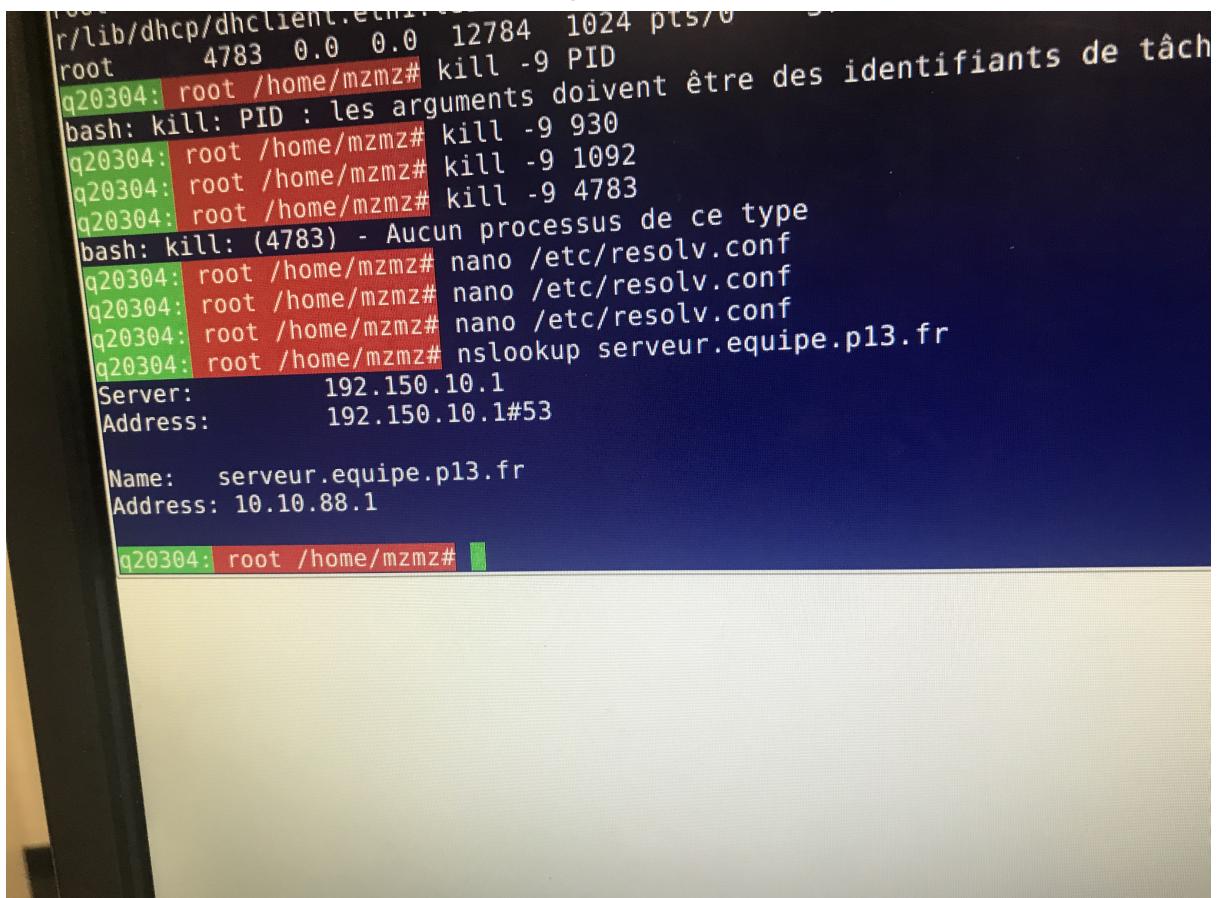
9)



On configure dans le fichier `/etc/resolv.conf` , et met l'adresse du serveur en changeant le domaine et search.

10- Tester depuis le PC client. Quelles commandes utilisez-vous ?

On utilise la commande nslookup



```
r/lib/dhcp/dhcclient.eth1: 4783 0.0 0.0 12784 1024 pts/0
root      4783 0.0 0.0 12784 1024 pts/0
q20304: root /home/mzmz# kill -9 PID
bash: kill: PID : les arguments doivent être des identifiants de tâche
q20304: root /home/mzmz# kill -9 930
q20304: root /home/mzmz# kill -9 1092
q20304: root /home/mzmz# kill -9 4783
bash: kill: (4783) - Aucun processus de ce type
q20304: root /home/mzmz# nano /etc/resolv.conf
q20304: root /home/mzmz# nano /etc/resolv.conf
q20304: root /home/mzmz# nano /etc/resolv.conf
q20304: root /home/mzmz# nslookup serveur.equipe.p13.fr
Server:      192.150.10.1
Address:      192.150.10.1#53

Name:  serveur.equipe.p13.fr
Address: 10.10.88.1

q20304: root /home/mzmz#
```

11- A l'aide de l'analyseur wireshark sur le PC client, regarder une requête DNS et sa

Réponse. Expliquez les champs observés.