

# TP DNS

Riboulet Célian S3B"

---

## 2) DHCP setup on LAN USER machines

In `/etc/network/interfaces` for dns1 dns2 client1 client2

```
iface eth0 inet dhcp
```

All addresses are set by the dhcp server on root

## 3) Adresses

```
dns1 : 192.168.0.1
dns2 : 192.168.0.2
client1 : 192.168.0.10
client2 : 192.168.0.20
```

## 4) Ping between LAN USER machines

```
(root@debian)-[~]
# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=0.889 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=1.45 ms
^C
--- 192.168.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.889/1.167/1.446/0.278 ms

(root@debian)-[~]
# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=1.48 ms
^C
--- 192.168.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.888/1.183/1.479/0.295 ms
```

## 5) Routing tables

```
(root@debian)-[~]
# route
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref     Use Iface
default          192.168.0.254   0.0.0.0          UG    0     0       0 eth0
192.168.0.0      0.0.0.0         255.255.255.0   U     0     0       0 eth0
```

## 7) Changing local host name

In **dns1** `/etc/hosts`

```
192.168.0.2      dns2
192.168.0.10    client1
192.168.0.20    client2
```

## 8) Ping using hostname

From dns1

```
(root@debian)-[~]
# ping dns2
PING dns2 (192.168.0.2) 56(84) bytes of data.
64 bytes from dns2 (192.168.0.2): icmp_seq=1 ttl=64 time=0.548 ms
64 bytes from dns2 (192.168.0.2): icmp_seq=2 ttl=64 time=1.47 ms
```

## 9) `/etc/resolv.conf`

Checking the file on all machines

```
GNU nano 3.4
nameserver 172.16.0.3
```

## 10) Forcing to use our own dns server

Editing `/etc/dhcp/dhclient.conf`

On **dns1** and **dns2** :

```
supersede domain-name-servers 127.0.0.1;
```

On **client1** :

```
supersede domain-name-servers 192.168.0.1;
```

On **client2** :

```
supersede domain-name-servers 192.168.0.2;
```

## 11) Restarting interfaces on all machines

After `ifdown eth0 && ifup eth0` the content of `/etc/resolv.conf` is now :

- for **dns1** and **dns2** :

- `nameserver 127.0.0.1`

- for **client1** :

- `nameserver 192.168.0.1`

- for **client2** :

- `nameserver 192.168.0.2`

## 12) DNS forwarding

`/etc/bind/named.conf.options` on **dns1** and **dns2** :

```
GNU nano 5.4
options {
    directory "/var/cache/bind";

    forwarders {
        172.16.0.3;
    };

    allow-query {
        any;
    };

    dnssec-validation no;

    // listen-on-v6 { any; };
};
```

## 13) Configuring primary server (dns1)

Add add a new dns zone on `/etc/bind/named.conf.local`

```
zone "netas" {  
    type master;  
    file "/etc/bind/db.netas";  
};
```

#### 14) Filling dns zone file

```
cp /etc/bind/db.empty /etc/bind/db.netas
```

#### 15) Updating zone file header

#### +16) Adding NS entry

```
/etc/bind/db.netas
```

```
$TTL      86400  
@         IN      SOA      dns1.netas. contact.netas. (  
                                1           ; Serial  
                                604800      ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                86400 )    ; Negative Cache TTL  
;  
@         IN      NS       localhost.  
@         IN      NS       dns1
```

#### 17) Adding A entry

```
/etc/bind/db.netas
```

```
@         IN      SOA      dns1.netas. contact.netas. (  
                                1           ; Serial  
                                604800      ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                86400 )    ; Negative Cache TTL  
;  
@         IN      NS       localhost.  
@         IN      NS       dns1  
dns1      IN      A        192.168.0.1
```

#### 18) Restarting the DNS service

```
systemctl restart named
```

We can also just reload the configuration without having to restart

```
systemctl reload named
```

Check possible errors with :

```
journalctl -u named
```

## 19) Checking status

To check the service status

```
systemctl status named
```

```
(root@debian)-[/etc/bind]
# systemctl status named
• named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; disabled; vendor preset: enabled)
  Active: active (running) since Tue 2022-01-04 14:48:46 CET; 2min 13s ago
    Docs: man:named(8)
  Main PID: 720 (named)
    Tasks: 5 (limit: 513)
  Memory: 13.2M
    CPU: 80ms
  CGroup: /system.slice/named.service
          └─720 /usr/sbin/named -f -4 -u bind

janv. 04 14:48:46 debian named[720]: managed-keys-zone: loading from master file managed-ke
janv. 04 14:48:46 debian named[720]: managed-keys-zone: loaded serial 2
janv. 04 14:48:46 debian named[720]: zone 0.in-addr.arpa/IN: loaded serial 1
janv. 04 14:48:46 debian named[720]: zone netas/IN: loaded serial 1
janv. 04 14:48:46 debian named[720]: zone 255.in-addr.arpa/IN: loaded serial 1
janv. 04 14:48:46 debian named[720]: zone 127.in-addr.arpa/IN: loaded serial 1
janv. 04 14:48:46 debian named[720]: zone localhost/IN: loaded serial 2
janv. 04 14:48:46 debian named[720]: all zones loaded
janv. 04 14:48:46 debian named[720]: running
janv. 04 14:48:46 debian named[720]: zone netas/IN: sending notifies (serial 1)
```

## 20) Ping from client to dns1 using its domain name

From client1

```
(root@debian)-[~]
# ping dns1.netas
PING dns1.netas (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=1 ttl=64 time=0.403 ms
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=2 ttl=64 time=1.53 ms
```

## 21) Adding A entry for dns2

The file is still `/etc/bind/db.netas`

```
$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        2      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        86400 )  ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
```

Dont forget to increment the Serial number and `systemctl reload named`

## 22) Adding `CNAME` entries (aliases)

```
$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        3      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        86400 )  ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
dns-primaire IN      CNAME  dns1
dns-secondaire IN     CNAME  dns2
```

<increment> Serial + `systemctl reload named`

## 23) Testing config from client

On client1

```

(root@debian)-[~]
# ping dns2.netas
PING dns2.netas (192.168.0.2) 56
64 bytes from 192.168.0.2 (192.168.0.2): icmp_seq=1 ttl=64 time=0.649 ms
64 bytes from 192.168.0.2 (192.168.0.2): icmp_seq=2 ttl=64 time=0.649 ms
^C
--- dns2.netas ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time=1000ms
rtt min/avg/max/mdev = 0.649/1.000/1.000/0.000 ms

(root@debian)-[~]
# ping dns-primaire.netas
PING dns1.netas (192.168.0.1) 56
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=2 ttl=64 time=0.368 ms
^C
--- dns1.netas ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time=1000ms
rtt min/avg/max/mdev = 0.368/0.800/0.800/0.000 ms

(root@debian)-[~]
# ping dns-secondaire.netas
PING dns2.netas (192.168.0.2) 56
64 bytes from 192.168.0.2 (192.168.0.2): icmp_seq=1 ttl=64 time=0.412 ms
^C
--- dns2.netas ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time=1000ms
rtt min/avg/max/mdev = 0.412/0.412/0.412/0.000 ms

```

## 24) Adding an `NS` entry to identify dns2 as a zone

`/etc/bind/db.netas`

```

$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        4           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        86400 )    ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
@         IN      NS       dns2
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
dns-primaire  IN    CNAME   dns1
dns-secondaire IN    CNAME   dns2

```

## 25) Setting up netas as secondary on dns2

On `/etc/bind/named.conf.local`

```
zone "netas" {
    type slave;
    file "/var/lib/bind/db.netas";
    masters { 192.168.0.1; };
};
```

## 26) Starting up DNS2 and checking with ping

```
systemctl restart named
```

Then on **client2** :

```
(root@debian)-[~]
# ping dns-primaire.netas
PING dns1.netas (192.168.0.1) 56(84) bytes of data:
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=1 ttl=64 time=0.577 ms
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=2 ttl=64 time=1.032 ms
^C
--- dns1.netas ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 0.001ms
rtt min/avg/max/mdev = 0.577/1.032/1.488/0.455 ms

(root@debian)-[~]
# ping dns2.netas
PING dns2.netas (192.168.0.2) 56(84) bytes of data:
64 bytes from 192.168.0.2 (192.168.0.2): icmp_seq=1 ttl=64 time=0.397 ms
64 bytes from 192.168.0.2 (192.168.0.2): icmp_seq=2 ttl=64 time=0.929 ms
^C
--- dns2.netas ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 0.001ms
rtt min/avg/max/mdev = 0.397/0.929/1.462/0.532 ms

(root@debian)-[~]
# ping dns1.netas
PING dns1.netas (192.168.0.1) 56(84) bytes of data:
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=1 ttl=64 time=0.577 ms
64 bytes from 192.168.0.1 (192.168.0.1): icmp_seq=2 ttl=64 time=1.032 ms
^C
```

## 27) Using `host` command on clients



```

(root@debian)-[~]
# host dns-primaire.netas 192.168.0.1
Using domain server:
Name: 192.168.0.1
Address: 192.168.0.1#53
Aliases:

dns-primaire.netas is an alias for dns1.netas.
dns1.netas has address 192.168.0.1

(root@debian)-[~]
# host dns-primaire.netas 192.168.0.2
Using domain server:
Name: 192.168.0.2
Address: 192.168.0.2#53
Aliases:

dns-primaire.netas is an alias for dns1.netas.
dns1.netas has address 192.168.0.1

(root@debian)-[~]
# host dns2.netas 192.168.0.2
Using domain server:
Name: 192.168.0.2
Address: 192.168.0.2#53
Aliases:

dns2.netas has address 192.168.0.2

```

## 28) Comparing dns2 and dns1 db.netas file

The file on dns2 seems to have the same content as dns1 but in another format (Compressed ?)

## 29) What is a /22 netmask

A /22 netmask is a mask has 22 bits dedicated to identify the network and the others are used to identify the computer.

192.168.0.(0-255)

192.168.1.(0-255)

192.168.2.(0-255)

192.168.3.(0-255)

## 30) Scanning the network to get all IPs

On dns1 :

```
nmap -T5 -sP 10.0.0.0/22
```

```
(root@debian)-[/etc/bind]
# nmap -T5 -sP 10.0.0.0/22
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-04 15:33 CET
Nmap scan report for 10.0.0.254
Host is up (0.00099s latency).
Nmap scan report for 10.0.1.1
Host is up (0.0015s latency).
Nmap scan report for 10.0.1.2
Host is up (0.0016s latency).
Nmap scan report for 10.0.2.1
Host is up (0.0016s latency).
Nmap scan report for 10.0.2.2
Host is up (0.0015s latency).
Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).
Nmap scan report for 10.0.3.1
Host is up (0.0016s latency).
Nmap scan report for 10.0.3.2
Host is up (0.0020s latency).
Nmap done: 1024 IP addresses (8 hosts up) scanned in 7.08 seconds
```

### 31) Connect over ssh to all found IPs

```
ssh tc@<ip>
```

10.0.0.254	root
10.0.1.1	a1
10.0.1.2	a2
10.0.2.1	s1
10.0.2.2	s2
10.0.2.3	s3
10.0.3.1	p1
10.0.3.2	p2

### 32) Add an A entry for s1 s2 and s3 web servers

```
/etc/bind/db.netas
```

```

$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        5_          ; Serial
                        604800       ; Refresh
                        86400        ; Retry
                        2419200      ; Expire
                        86400 )      ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
@         IN      NS       dns2
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
s1        IN      A        10.0.2.1
s2        IN      A        10.0.2.2
s3        IN      A        10.0.2.3
dns-primaire IN      CNAME  dns1
dns-secondeaire IN    CNAME  dns2

```

Serial number bumped up to 5

```
systemctl restart named
```

### 33) Add a `CNAME` entry for the 3 web servers

```

$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        6           ; Serial
                        604800       ; Refresh
                        86400        ; Retry
                        2419200      ; Expire
                        86400 )      ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
@         IN      NS       dns2
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
s1        IN      A        10.0.2.1
s2        IN      A        10.0.2.2
s3        IN      A        10.0.2.3
dns-primaire IN      CNAME  dns1
dns-secondeaire IN    CNAME  dns2
creative   IN      CNAME  s1
grayscale  IN      CNAME  s2
wonder     IN      CNAME  s3

```

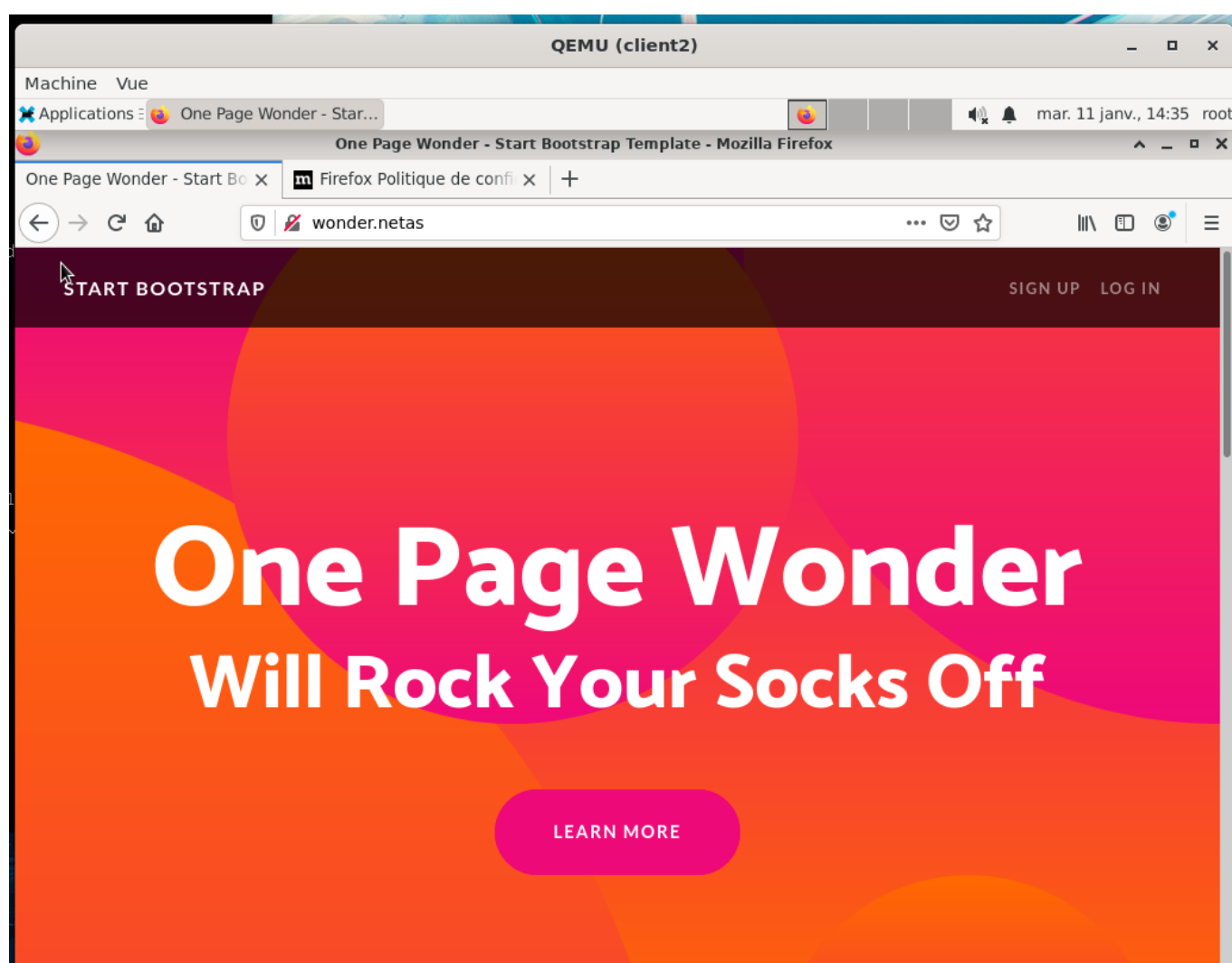
### 34) Test from client1 and client2

```
(root@debian)-[~]
# ping grayscale.netas
PING s2.netas (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2 (10.0.2.2): icmp_seq=1 ttl=63 time=0.887 ms
^C
--- s2.netas ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.887/0.887/0.887/0.000 ms

(root@debian)-[~]
# ping wonder.netas
PING s3.netas (10.0.2.3) 56(84) bytes of data.
64 bytes from 10.0.2.3 (10.0.2.3): icmp_seq=1 ttl=63 time=1.20 ms
^C
--- s3.netas ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.198/1.198/1.198/0.000 ms
```

35) 36) 37) Start web browser on client 1 and then client2

startx



### 38) Declaring inverse domain name zone for netas

```
/etc/bind/named.conf.local on dns1
```

```
zone "2.0.10.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.netas-rev;  
};
```

```
/etc/bin/db.netas-rev
```

```
$TTL      86400  
@         IN      SOA      dns1.netas. contact.netas. (  
                                2          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                86400 )    ; Negative Cache TTL  
;  
@         IN      NS       dns1.netas.  
@         IN      NS       dns2.netas.  
1         IN      PTR      s1.netas.  
2         IN      PTR      s2.netas.  
3         IN      PTR      s3.netas.
```

### 39) Check on client if the reverse domain name is working

On client2

```
(root@debian)-[~]  
# host 10.0.2.1  
1.2.0.10.in-addr.arpa domain name pointer s1.netas.
```

### 40) Update dns2 configuration

In order for dns2 to become a secondary server on the reverse netas zone

```
/etc/bind/named.conf.local
```

```

zone "netas" {
    type slave;
    file "/var/lib/bind/db.netas";
    masters { 192.168.0.1; };
};

zone "2.0.10.in-addr.arpa" {
    type slave;
    file "/var/lib/bind/db.netas-rev";
    masters { 192.168.0.1; };
};

```

#### 41) Testing on client2

```

(root@debian)-[~]
# host 10.0.2.1
;; connection timed out; no servers could be reached

(root@debian)-[~]
# host 10.0.2.1
1.2.0.10.in-addr.arpa domain name pointer s1.netas.

```

Before and after the setup

#### 42) Add new NS entry to the netas zone (subdomain setup)

```

$TTL      86400
@         IN      SOA      dns1.netas. contact.netas. (
                        7      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        86400 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      NS       dns1
@         IN      NS       dns2
dns1      IN      A        192.168.0.1
dns2      IN      A        192.168.0.2
s1        IN      A        10.0.2.1
s2        IN      A        10.0.2.2
s3        IN      A        10.0.2.3
dns-primaire IN    CNAME    dns1
dns-secondaire IN  CNAME    dns2
creative  IN      CNAME    s1
grayscale IN      CNAME    s2
wonder    IN      CNAME    s3
perf      IN      NS       dns1

```

### 43) Declaring the new subdomain

/etc/bind/named.conf.local

```
zone "netas" {
    type master;
    file "/etc/bind/db.netas";
};

zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.netas-rev";
};

zone "perf.netas" {
    type master;
    file "/etc/bind/db.perf.netas";
};_
```

### 44) Creating zone file

/etc/bind/db.perf.netas

```
$TTL      86400
@         IN      SOA      dns1.perf.netas. contact.netas. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400 )    ; Negative Cache TTL
;
@         IN      NS       dns1
dns1      IN      A        192.168.0.1
```

### 45) Adding A entries for p1 and p2

```
$TTL      86400
@         IN      SOA      dns1.perf.netas. contact.netas. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400 )    ; Negative Cache TTL
;
@         IN      NS       dns1
dns1      IN      A        192.168.0.1
p1        IN      A        10.0.3.1
p2        IN      A        10.0.3.2
```

### 46) Check on client1

```
(root@debian)-[~]  
# host p1.perf.netas  
p1.perf.netas has address 10.0.3.1
```

#### 47) Share A between p1 and p2

```
$TTL      86400  
@         IN      SOA      dns1.perf.netas. contact.netas. (  
          3_        ; Serial  
          604800     ; Refresh  
          86400      ; Retry  
          2419200    ; Expire  
          86400 )    ; Negative Cache TTL  
;  
@         IN      NS       dns1  
dns1      IN      A        192.168.0.1  
p1        IN      A        10.0.3.1  
p2        IN      A        10.0.3.2  
scale     IN      A        10.0.3.1  
scale     IN      A        10.0.3.2
```

#### 48) Pinging scale.perf.netas on client1

The pinged IP does change randomly between the p1 and p2 IPs

#### 49) Installing iperf on client1 and client2

```
(root@debian)-[~]  
# apt install iperf  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
iperf est déjà la version la plus récente (2.0.14a+dfsg1-1).  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

#### 50) Updating dns1 and dns2 so dns2 is a secondary server on the perf.netas zone

named.conf.local on DNS2



```

zone "netas" {
    type slave;
    file "/var/lib/bind/db.netas";
    masters { 192.168.0.1; };
};

zone "2.0.10.in-addr.arpa" {
    type slave;
    file "/var/lib/bind/db.netas-rev";
    masters { 192.168.0.1; };
};

zone "perf.netas" {
    type slave;
    file "/var/lib/bind/db.perf.netas";
    masters { 192.168.0.1; };
};

```

### 51) Ping from client2

```

(root@debian)-[~]
# ping scale.perf.netas
PING scale.perf.netas (10.0.3.1) 56(84) bytes of data.
64 bytes from 10.0.3.1 (10.0.3.1): icmp_seq=1 ttl=63 time=1.38 ms
64 bytes from 10.0.3.1 (10.0.3.1): icmp_seq=2 ttl=63 time=2.58 ms
^C

```

### 52) Speed test on client1 & client2

```

(root@debian)-[~]
# iperf -t 5 -c scale.perf.netas
-----
Client connecting to scale.perf.netas, TCP port 5001
TCP window size: 153 KByte (default)
-----
[ 3] local 192.168.0.10 port 34190 connected with 10.0.3.2 port 5001
client await server close failed: Resource temporarily unavailable
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0000-5.0249 sec 159 MBytes 266 Mbits/sec

```

### 53)