TP6 : Des bo services dans des bo LANs

I. Le setup

⬡ Prouvez que...

- une machine du LAN1 peut joindre internet (ping un nom de domaine)

```
[dylan@dns ~]$ ping ynov.com
PING ynov.com (104.26.11.233) 56(84) bytes of data.
64 bytes from 104.26.11.233 (104.26.11.233): icmp_seq=1 ttl=53 time=18.3 ms
64 bytes from 104.26.11.233 (104.26.11.233): icmp_seq=2 ttl=53 time=17.2 ms
64 bytes from 104.26.11.233 (104.26.11.233): icmp_seq=3 ttl=53 time=18.3 ms
64 bytes from 104.26.11.233 (104.26.11.233): icmp_seq=4 ttl=53 time=17.6 ms
^C
--- ynov.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 17.200/17.844/18.302/0.462 ms
```

- une machine du LAN2 peut joindre internet (ping nom de domaine)`

```
[dylan@dhcp ~]$ ping ynov.com
PING ynov.com (104.26.10.233) 56(84) bytes of data.
64 bytes from 104.26.10.233 (104.26.10.233): icmp_seq=1 ttl=53 time=17.3 ms
64 bytes from 104.26.10.233 (104.26.10.233): icmp_seq=2 ttl=53 time=17.0 ms
^C64 bytes from 104.26.10.233: icmp_seq=3 ttl=53 time=18.5 ms

--- ynov.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 16.962/17.590/18.544/0.685 ms
```

- une machine du LAN1 peut joindre une machine du LAN2 (ping une adresse IP)

```
[dylan@dns ~]$ ping  10.6.1.253
PING 10.6.1.253 (10.6.1.253) 56(84) bytes of data.
64 bytes from 10.6.1.253: icmp_seq=1 ttl=63 time=2.05 ms
64 bytes from 10.6.1.253: icmp_seq=2 ttl=63 time=2.07 ms
64 bytes from 10.6.1.253: icmp_seq=3 ttl=63 time=1.78 ms
64 bytes from 10.6.1.253: icmp_seq=4 ttl=63 time=1.57 ms
^C
--- 10.6.1.253 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.570/1.866/2.070/0.205 ms
```

II. LAN clients

⬡ Prouvez que...

- le client a bien récupéré une adresse IP en DHCP

```
[dylan@client1 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:37:5f:3a brd ff:ff:ff:ff:ff:ff
    ⬡inet 10.6.1.37/24 brd 10.6.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 43069sec preferred_lft 43069sec
    inet6 fe80::a00:27ff:fe37:5f3a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- vous avez bien 1.1.1.1 en DNS

```
[dylan@client1 ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 1.1.1.1
```

- vous avez bien la bonne passerelle indiquée

```
[dylan@client1 ~]$ ip r s
default via 10.6.1.254 dev enp0s3 proto dhcp src 10.6.1.37 metric 100
10.6.1.0/24 dev enp0s3 proto kernel scope link src 10.6.1.37 metric 100
```

- que ça ping un nom de domaine public sans problème magueule

```
[dylan@client1 ~]$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=53 time=17.3 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=53 time=17.0 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=53 time=17.4 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=53 time=18.2 ms
^C
--- 1.1.1.1 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 17.028/17.456/18.188/0.438 ms
```

III. LAN serveurzzzz

1. Serveur Web

⬡ Déterminer sur quel port écoute le serveur NGINX

```
[dylan@web ~]$ sudo ss -lnpt | grep 80
LISTEN 0      511          0.0.0.0:80         0.0.0.0:*    users:
(("nginx",pid=1503,fd=6),("nginx",pid=1502,fd=6))
LISTEN 0      511             [::]:80            [::]:*    users:
(("nginx",pid=1503,fd=7),("nginx",pid=1502,fd=7))
```

⬡ Ouvrir ce port dans le firewall

```
[dylan@web ~]$ sudo firewall-cmd --permanent --add-port=80/tcp
success
[dylan@web ~]$ sudo firewall-cmd --reload
success
```

⬡ Visitez le site web !

```
[dylan@client1 ~]$ curl http://10.6.2.11
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
```

2. Serveur DNS

⬡ Déterminer sur quel(s) port(s) écoute le service BIND9

```
[dylan@dns ~]$ sudo ss -lnpt | grep 53
LISTEN 0      10         10.6.1.12:53         0.0.0.0:*    users:
(("named",pid=1914,fd=22))
```

⬡ Ouvrir ce(s) port(s) dans le firewall

```
[dylan@dns ~]$ sudo firewall-cmd --permanent --add-port=53/tcp
success
[dylan@dns ~]$
[dylan@dns ~]$ sudo firewall-cmd --reload
success
```

◯ Effectuez des requêtes DNS manuellement depuis le serveur DNS lui-même dans un premier temps

```
[dylan@dns ~]$ dig web.tp6.b1 @10.6.2.12

; <<>> DiG 9.16.23-RH <<>> web.tp6.b1 @10.6.2.12
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17062
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 21a6e878def8d92601000000671667f5a2525912ff789e65 (good)
;; QUESTION SECTION:
;web.tp6.b1.                       IN      A

;; ANSWER SECTION:
web.tp6.b1.            86400   IN      A       10.6.2.11

;; Query time: 0 msec
;; SERVER: 10.6.2.12#53(10.6.2.12)
;; WHEN: Mon Oct 21 16:40:53 CEST 2024
;; MSG SIZE  rcvd: 83
```

```
[dylan@dns ~]$ dig -x 10.6.2.11 @10.6.2.12

; <<>> DiG 9.16.23-RH <<>> -x 10.6.2.11 @10.6.2.12
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20672
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d7aae2ca8478044101000000671668caa56bc07e57d95d8f (good)
;; QUESTION SECTION:
;11.2.6.10.in-addr.arpa.              IN      PTR

;; ANSWER SECTION:
11.2.6.10.in-addr.arpa. 86400   IN      PTR     web.tp6.b1.

;; Query time: 11 msec
```

```
;; SERVER: 10.6.2.12#53(10.6.2.12)
;; WHEN: Mon Oct 21 16:44:26 CEST 2024
;; MSG SIZE  rcvd: 103
```

◯ Effectuez une requête DNS manuellement depuis client1.tp6.b1

```
[dylan@client1 ~]$ dig web.tp6.b1 @10.6.2.12

; <<>> DiG 9.16.23-RH <<>> web.tp6.b1 @10.6.2.12
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14493
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 346c2b77e79fcfbb0100000067166a88532f904db74236b6 (good)
;; QUESTION SECTION:
;web.tp6.b1.                    IN      A

;; ANSWER SECTION:
web.tp6.b1.             86400   IN      A       10.6.2.11

;; Query time: 12 msec
;; SERVER: 10.6.2.12#53(10.6.2.12)
;; WHEN: Mon Oct 21 16:51:52 CEST 2024
;; MSG SIZE  rcvd: 83
```

3. Serveur DHCP

◯ Créez un nouveau client client2.tp6.b1 vitefé

récupérez une IP en DHCP sur ce nouveau client2.tp6.b1

```
[dylan@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:bf:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 10.6.1.38/24 brd 10.6.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 43121sec preferred_lft 43121sec
    inet6 fe80::a00:27ff:febf:b887/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

vérifiez que vous avez bien 10.6.2.12 comme serveur DNS à contacter

```
[dylan@localhost ~]$ sudo cat /etc/resolv.conf
[sudo] password for dylan:
# Generated by NetworkManager
nameserver 10.6.2.12
```

```
[dylan@localhost ~]$ curl http://web.tp6.b1
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
```