

Rapport de TP en Groupe

VIGAN Silas

11 avril 2017

1 Import des différents Equipements dans l'environnement de travail

Dans le but de pouvoir utiliser les équipements d'interconnexion, il est important que nous importons ces équipements dans notre environnement de travail afin de pouvoir simuler le monde réel de travail.

1.1 Import de routeur MikroTik

Nous avons d'abord importé un routeur MikroTik. Pour ce faire,

Dans GNS3 nous avons ouvert la fenêtre des préférences : **Edit > Preferences**, Dans cette fenêtre nous avons choisi **Qemu VMs** dans le volet de gauche. Puis nous avons cliqué sur **New**, donné un nom à notre modèle de routeur dans la zone **Name** de la fenêtre **New Qemu VM Template**. Nous avons cliqué deux fois sur Next. Dans la partie **Disk image(hda)**, nous avons cliqué sur Browse et navigué à l'emplacement de notre image pour choisir le fichier mk6.img. Nous avons cliqué enfin sur Finish. Un nouvel équipement portant le nom que nous avons défini apparaît dans le volet central.

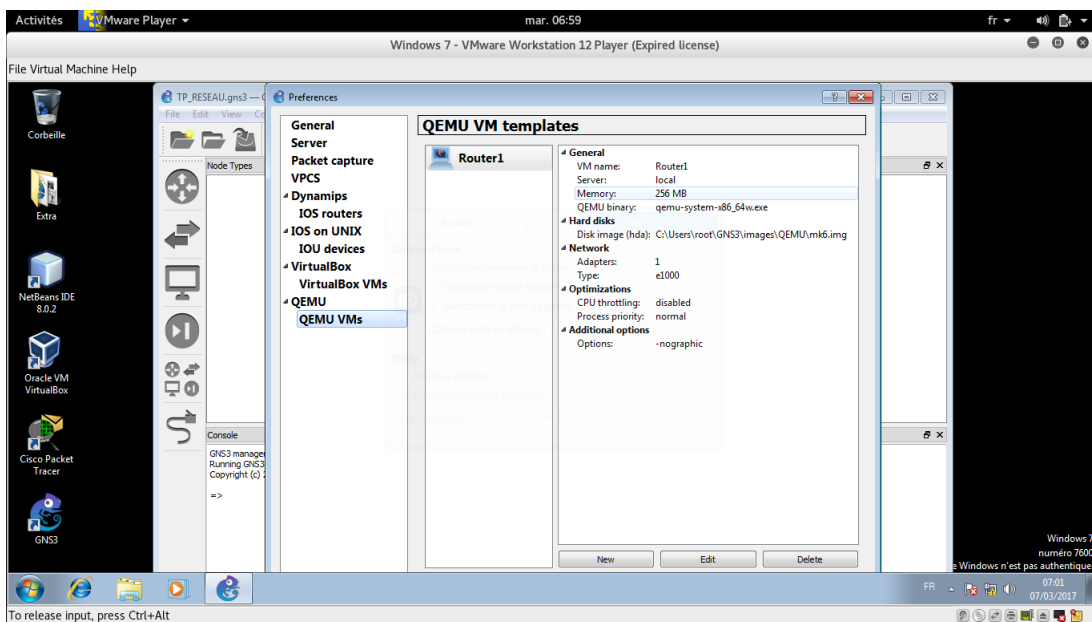


FIGURE 1 – Importation du routeur MikroTik

1.2 Import de routeur Cisco

Cisco Pour importer un routeur cisco Dans GNS3 nous avons ouvert la fenêtre des préférences : **Edit > Preferences**, Dans cette fenêtre nous avons choisi **IOS routers** dans le volet de gauche sous **Dynamips**. Puis cliqué sur **New**. Dans la partie **IOS image**, nous avons ensuite cliqué sur **Browse** et navigué à l'emplacement de notre image pour choisi le fichier .image ou .bin de Cisco. Nous avons cliqué ensuite sur Next 3 fois de suite puis sur Finish

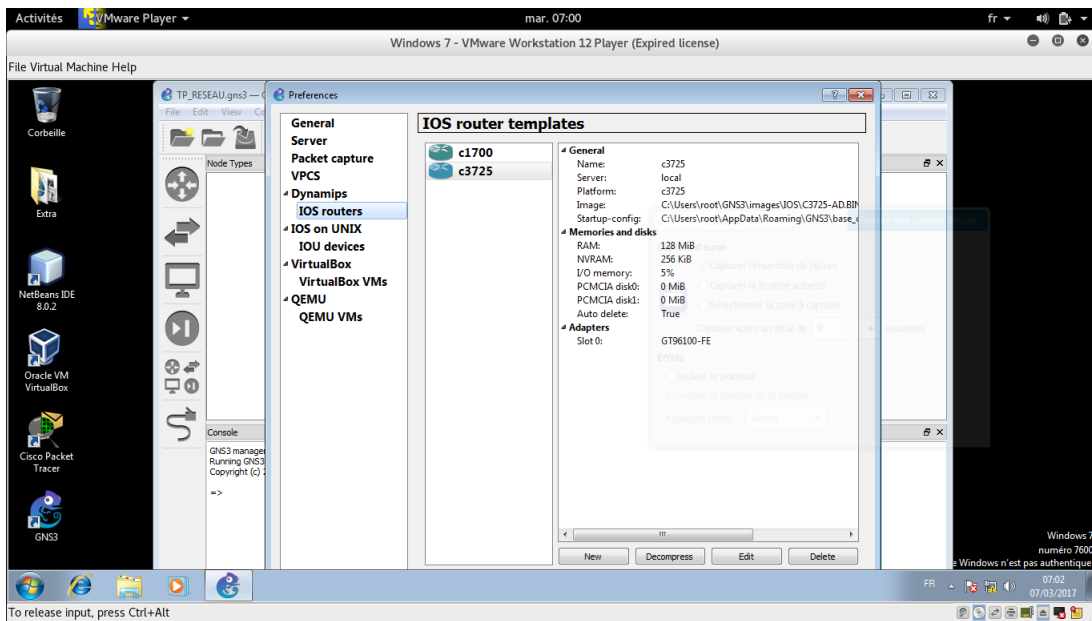


FIGURE 2 – Importation du routeur Cisco

2 Mise en Place de l'architecture

Dans notre simulateur, nous allons mettre en place l'architecture

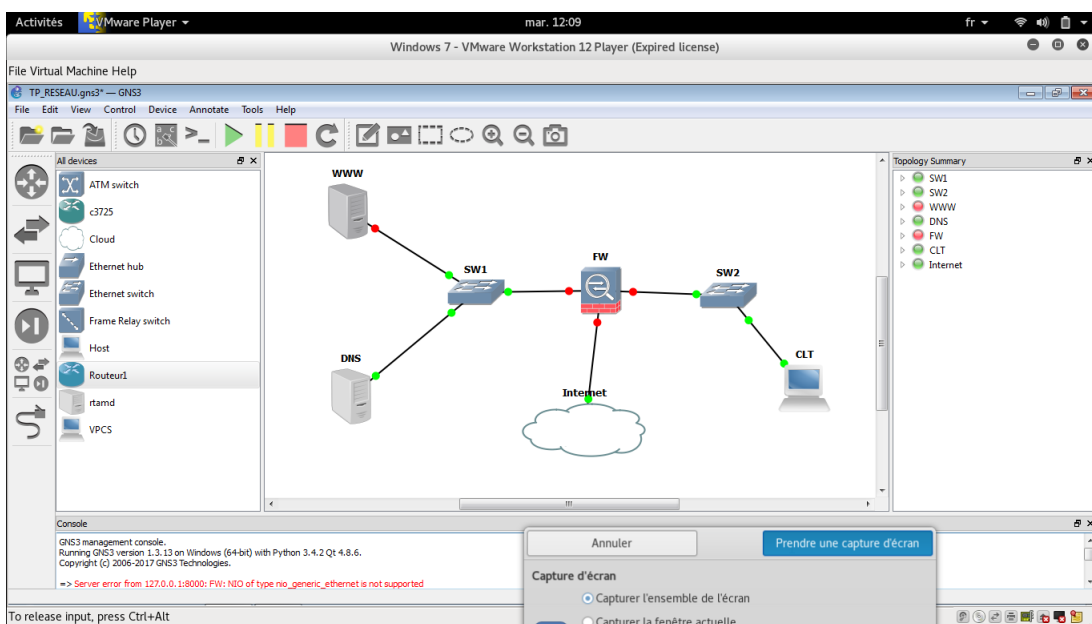


FIGURE 3 – Architecture du TP

3 Activités

3.1 Activité 1 : passerelle et firewall

Notre première activité consistera en la configuration du routeur FW :

3.1.1 Activation du forwarding sur le serveur FW

On édite le fichier /etc/sysctl.conf/. Puis on modifie la ligne portant net.ipv4 forward en mettant sa valeur à 1.

3.1.2 Configuration de la règle Iptable pour définir le NAT sur l'interface eth2 en sortie

```
iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -d 192.168.4.0/24 -o eth2 -j MASQUARADE
```

3.1.3 Configuration de règles iptable sur FW pour :

a- toutes les règles de filtrages sur le routeur FW :

```
iptables -F
```

b- N'autoriser que les requête HTTP vers le serveur Web :

```
iptables -A FORWARD -s 192.168.3.0/24 -d 193.165.20.2 -p tcp --dport 80 -j ACCEPT
```

c- N'autoriser les requêtes FTP vers le serveur web que si elles proviennent du réseau 192.168.3.0/24

```
iptables -A FORWARD -s 192.168.3.0/24 -d 193.165.20.2 -p tcp --dport 21 -j ACCEPT
```

d- Autoriser les requêtes vers les autres services abrités par les différents serveurs

```
iptables -A FORWARD -s 192.168.3.0/24 -d 193.165.20.0/24 -p tcp -j ACCEPT
```

e- Droppez tous les paquets icmp en provenance de la machine CLT (192.168.3.2) et ajoutez un message d'alerte au log /var/log/messages

```
iptables -A FORWARD -p icmp -s 192.168.3.2 -j LOG
```

```
iptables -t filter -A FORWARD -p icmp -s 192.168.3.2 -j DROP
```

3.1.4 CATCH ALL rules

```
iptables -A FORWARD -j DROP
```

```
iptables -A FORWARD -j LOG
```

3.2 Activité 2

3.2.1 Configuration du routeur FW comme passerelle vers Internet en le connectant à un cloud associé à votre carte réseau qui est connectée à internet

3.2.2 Configuration du service DHCP sur ce routeur pour son interface connectée au LAN

Dans le fichier /etc/default/isc-dhcp-server, modifier INTERFACES= "" par INTERFACES= "eth0"

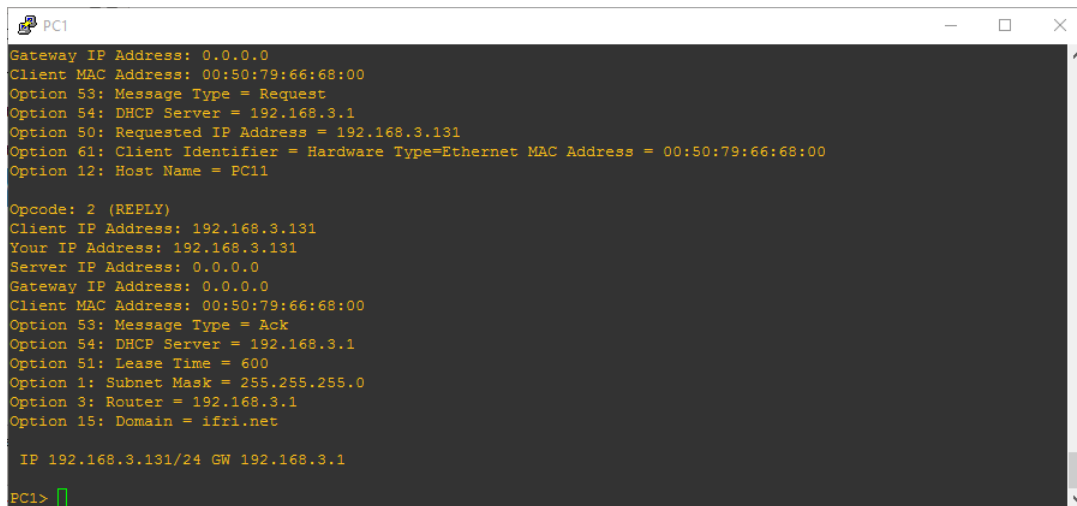
3.2.3 Définissons au niveau du routeur

a- le pool DHCP en réservant une trentaine d'adresses IP pour un usage futur

Dans le fichier /etc/dhcp/dhcpd.conf :

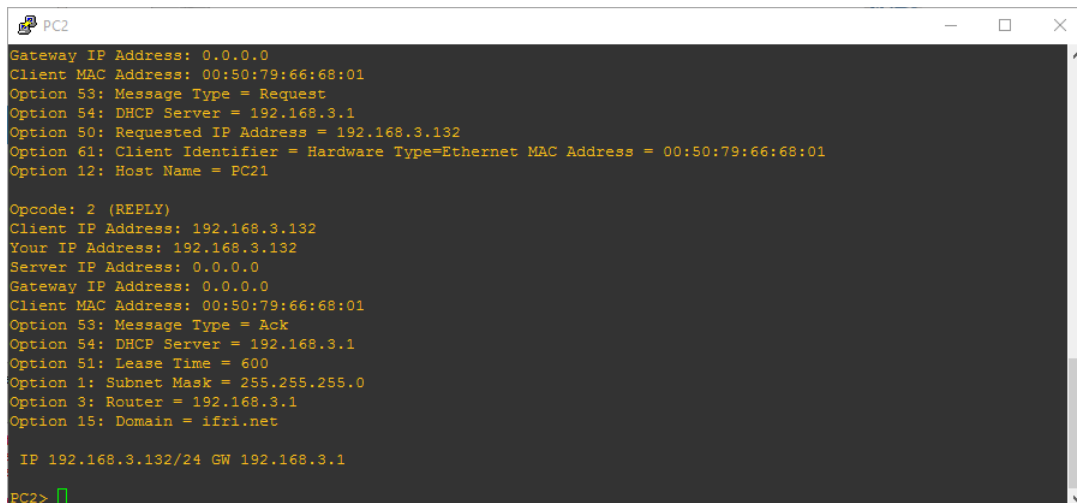
```
subnet 192.168.3.0 netmask 255.255.255.0 {  
    range 192.168.3.128 192.168.3.254;option routers 192.168.3.1;  
    option broadcast-address 192.168.3.255;  
    ddns-domainname "ifri.net";  
    option domain-name "ifri.net"; }
```

3.2.4 Test de fonctionnement



```
PC1  
Gateway IP Address: 0.0.0.0  
Client MAC Address: 00:50:79:66:68:00  
Option 53: Message Type = Request  
Option 54: DHCP Server = 192.168.3.1  
Option 50: Requested IP Address = 192.168.3.131  
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:00  
Option 12: Host Name = PC11  
  
Opcode: 2 (REPLY)  
Client IP Address: 192.168.3.131  
Your IP Address: 192.168.3.131  
Server IP Address: 0.0.0.0  
Gateway IP Address: 0.0.0.0  
Client MAC Address: 00:50:79:66:68:00  
Option 53: Message Type = Ack  
Option 54: DHCP Server = 192.168.3.1  
Option 51: Lease Time = 600  
Option 1: Subnet Mask = 255.255.255.0  
Option 3: Router = 192.168.3.1  
Option 15: Domain = ifri.net  
  
IP 192.168.3.131/24 GW 192.168.3.1  
PC1> █
```

FIGURE 4 – Résultat sur le PC1



```
PC2  
Gateway IP Address: 0.0.0.0  
Client MAC Address: 00:50:79:66:68:01  
Option 53: Message Type = Request  
Option 54: DHCP Server = 192.168.3.1  
Option 50: Requested IP Address = 192.168.3.132  
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:01  
Option 12: Host Name = PC21  
  
Opcode: 2 (REPLY)  
Client IP Address: 192.168.3.132  
Your IP Address: 192.168.3.132  
Server IP Address: 0.0.0.0  
Gateway IP Address: 0.0.0.0  
Client MAC Address: 00:50:79:66:68:01  
Option 53: Message Type = Ack  
Option 54: DHCP Server = 192.168.3.1  
Option 51: Lease Time = 600  
Option 1: Subnet Mask = 255.255.255.0  
Option 3: Router = 192.168.3.1  
Option 15: Domain = ifri.net  
  
IP 192.168.3.132/24 GW 192.168.3.1  
PC2> █
```

FIGURE 5 – Résultat sur le PC2

4 Activité : Serveurs DNS et Mail

4.1 Editons le fichier de configuration (/etc/bind/named.conf.local) et déclarons convenablement (type et fichier de zone) les zones :

- ifri.net
- 3.168.192.in-addr.arpa
- 20.165.193.in-addr.arpa

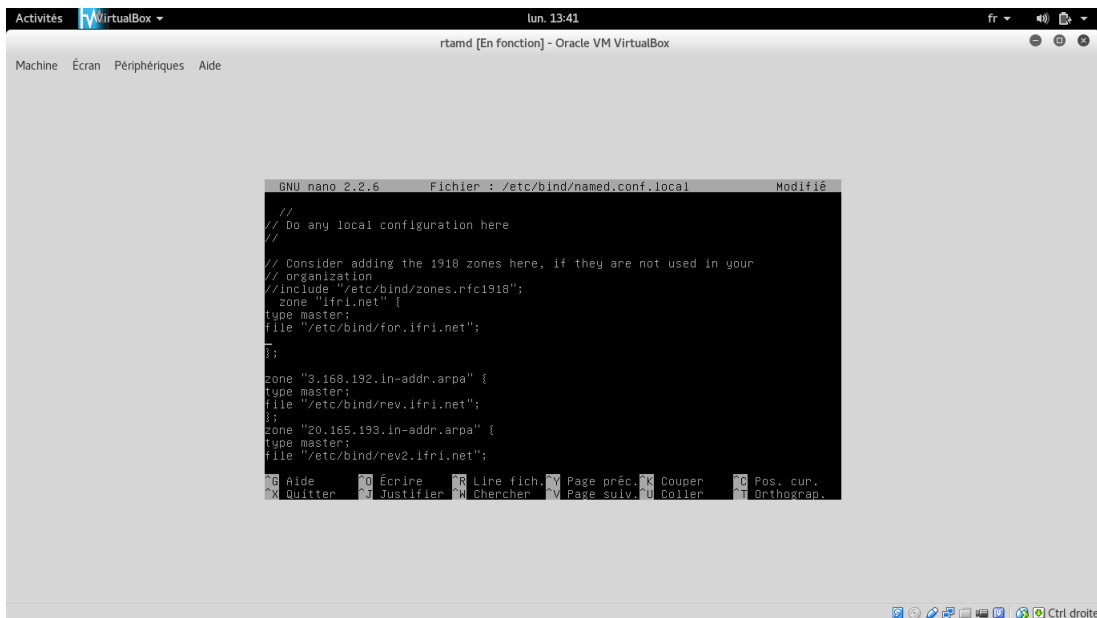


FIGURE 6 – Configuration des zones dans le fichier **named.conf.local**

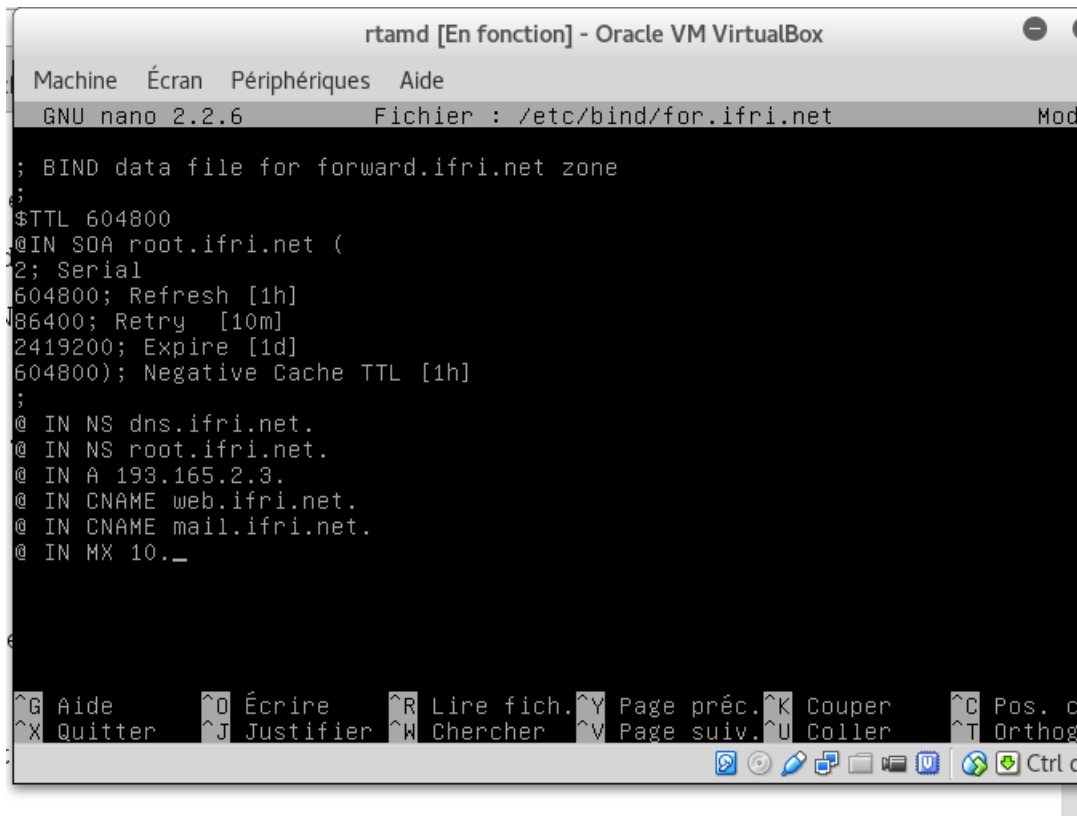
4.2 Création des fichiers de zones préalablement déclarés



FIGURE 7 – Création des fichiers de zones

4.3 Création des enregistrements de ressources ci-après sur le serveur DNS faisant autorité pour le domaine ifri.net :

- **type=NS** déclarant le serveur lui meme comme faisant autorité pour le domaine ifri.net
- **type=NS** déclarant le second serveur comme slave pour le domaine ifri.net
- **type=A** déclarant l'adresse IP des serveurs de nom de domaine(c'est l'adresse de chaque serveur)
- **type=CNAME** déclarant un alias web pointant sur le serveur web
- **type=CNAME** déclarant un alias mail pointant sur le serveur mail
- **type=MX** déclarant le serveur comme le serveur smtp(mail) du do- maine ifri.net avec priorité 10



The screenshot shows a terminal window titled "rtamd [En fonction] - Oracle VM VirtualBox". The terminal is running GNU nano 2.2.6, editing the file "/etc/bind/forward.ifri.net". The content of the file is as follows:

```
; BIND data file for forward.ifri.net zone
;
$TTL 604800
@IN SOA root.ifri.net (
2; Serial
604800; Refresh [1h]
86400; Retry [10m]
2419200; Expire [1d]
604800); Negative Cache TTL [1h]
;
@ IN NS dns.ifri.net.
@ IN NS root.ifri.net.
@ IN A 193.165.2.3.
@ IN CNAME web.ifri.net.
@ IN CNAME mail.ifri.net.
@ IN MX 10._
```

The terminal window also shows a menu bar with options like Aide, Écrire, Lire fich., Page préc., Couper, Pos. c, and a status bar with various icons and keyboard shortcuts.

FIGURE 8 – Création des enrégistrement de ressources