

Travaux Pratiques N° 3

Configuration d'un réseau de machines virtuelles — Utilisation de Wireshark

Un rapport est à remettre en déposant une archive compressée dans la zone de dépôt des travaux.

Exercice 1 (Configuration d'un réseau de machines virtuelles)

Vous disposez de trois machines virtuelles qui sont organisées en réseau comme représenté par la figure 1.

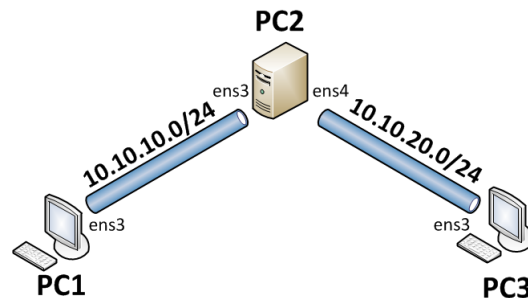


FIGURE 1 – Schéma de l'architecture réseau

1) Afin d'accéder aux machines virtuelles, ouvrez un navigateur et saisissez l'URL suivante :

<http://194.57.105.124/vnc.html>

2) Après avoir cliqué l'icône **Settings**, comme indiqué sur la figure (2), supprimez le texte dans le champ "**Path**" et sélectionnez le mode "**Local Scaling**" dans le champ "**Scaling Mode**".

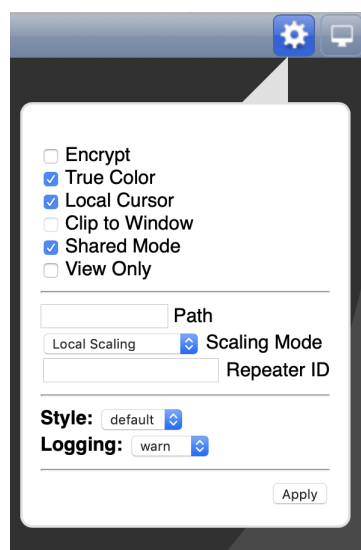


FIGURE 2 – Réglage du navigateur pour accéder aux machines virtuelles

3) Pour accéder à la machine virtuelle PC1, cliquez l'icône [connect], comme indiqué sur la figure (3), ensuite renseignez dans le champ "**Port**" le numéro du port "**69xx**" en remplaçant "**xx**" par le numéro donné par votre intervenant. Soit P ce numéro de port.

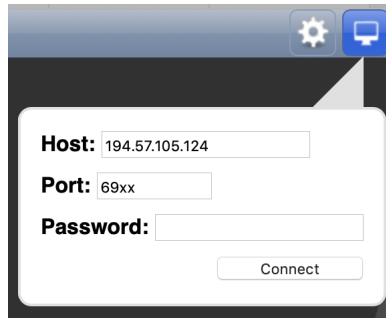


FIGURE 3 – Formuler un accès une machine virtuelle

Maintenant, vous ouvrez un onglet dans votre navigateur web par machine virtuelle. Reprenez la procédure précédente pour accéder à la machine PC2, respectivement PC3 en utilisant le port $P + 1$, respectivement $P + 2$.

Maintenant que vous êtes connectés à vos trois machines virtuelles, nous allons procéder à leur configuration. Pour cela, nous allons commencer par la configuration du PC1.

4) À chaque début de TP, pensez à redémarrer chacune des trois machines virtuelles afin de réinitialiser les réglages réseaux de toutes les machines renseignés par les autres étudiants qui vous ont précédé.

5) Après avoir redémarré le PC1, connectez-vous au compte utilisateur :

- Login : toto
- Mot de passe : toto

6) Ouvrez un terminal et passez en mode super-utilisateur :

```
$> sudo su
```

7) Consultez le manuel de la commande ip :

```
$> man ip
```

8) Consultez la liste des interfaces réseaux disponibles :

```
$> ip a show
```

Pour obtenir un affichage à contexte coloré, utilisez l'option :

```
$> ip -c a show
```

9) Modifiez l'adresse IP de l'interface "ens3" afin de correspondre au schéma de la figure 1 :

```
$> ip a add <adresse-ip>/<masque> dev <interface>
```

10) Activez l'interface réseau "ens3" :

```
$> ip link set up dev <interface>
```

11) Faites la même configuration pour la machine PC3 afin de correspondre au schéma de la figure 1.

Maintenant, nous allons configurer la machine PC2 comme passerelle entre PC1 et PC3.

12) Après avoir redémarré le PC2, connectez-vous au compte super-utilisateur :

- Login : root
- Mot de passe : toor

13) Consultez la liste des interfaces réseau disponibles.

14) Quelle devrait être l'adresse IP de l'interface "ens3" de la machine PC2 ? Assignez donc cette adresse IP à cette interface. Activez l'interface "ens3".

15) Quelle devrait être l'adresse IP de l'interface "ens4" de la machine PC2 ? Assignez donc cette adresse IP à cette interface. Activez l'interface "ens3".

Revenons maintenant à la machine PC1 pour tester les connexions entre les trois machines PC1, PC2 et PC3.

16) Depuis la machine PC1, lancez l'outil *Wireshark*. Ensuite, démarrez la capture des trames ethernet sur l'interface "ens3".

17) À partir de la machine PC3, envoyez un ping vers l'interface de PC2 qui est dans le même sous-réseau que PC1. Est-ce que la communication fonctionne ?

18) Arrêtez la capture dans *Wireshark* et interprétez les datagrammes des paquets *ICMP* et *ARP*.

19) Après avoir redémarré la capture dans "*Wireshark*", envoyez à partir de PC3 un ping vers PC2. Est-ce que la communication fonctionne ? Interprétez les datagrammes des paquets *ICMP* et *ARP*.

20) Après avoir redémarré la capture dans "*Wireshark*", envoyez à partir de PC1 un ping vers PC3. Est-ce que la communication fonctionne ? Interprétez les datagrammes des paquets *ICMP* et *ARP*.

21) Comment pourrait-on résoudre cette situation ?

22) Rajoutez l'adresse de la passerelle dans PC3 :

```
$> ip r add default via <adresse-ip-gateway>
```

23) En enregistrant les trames sur *Wireshark*, testez la communication entre PC1 et l'interface de PC2 qui est dans le même sous-réseau que PC3. Est-ce que la communication fonctionne ?

24) En enregistrant les trames sur *Wireshark*, testez la communication entre PC1 et PC3. Est-ce que la communication fonctionne ? Comment pourrait-on résoudre cette situation ?

25) Après avoir modifié la configuration de PC3 de la même manière que pour PC1, testez la communication entre PC1 et PC3. Est-ce que la communication fonctionne ? Comment pourrait-on résoudre cette solution ?

26) Il faut alors revenir sur PC2 afin d'activer le relayage (*forwarding*) IP. Pour cela, tapez cette commande shell :

```
$> sysctl -w net.ipv4.conf.all.forwarding="1"
```

27) Vérifiez que cette modification a été bien prise en compte :

```
$> cat /proc/sys/net/ipv4/ip_forward
```

28) Testez maintenant la communication entre PC1 et PC3. Est-ce que la communication fonctionne ?

Exercice 2 (Capturez vos trames !)

Une fois que les machines virtuelles sont correctement configurées, vous allez vérifier leurs capacités à communiquer. Pour cela, lancez l'analyseur de réseau *Wireshark* (mode super utilisateur) et filtrez les captures des trames échangées entre les machines "PC1" et "PC3", particulièrement celles qui concernent des scénarios de communications en utilisant des services tels :

- telnet
- ssh
- ftp
- sftp

- 1) Analysez les trames capturées :
- séquences d'ouverture de connexion,
 - séquences d'échanges de données volumineuses
 - séquences de clôture de connexions

Admettons que l'on utilise le scénario suivant :

```
toto@PC1:/home/toto> telnet PC3
Trying ....
Connected to ...
Escape character is '^]'.
Ubuntu 16.04.6 LTS
Ubuntu login:
...
...
...
```

- 2) Quelles sont les adresses MAC renseignées dans les trames capturées ?
- 3) Pour quelle raison ne voit on jamais apparaître dans les trames ethernet l'adresse MAC de la machine PC3 ?
- 4) Repérez la trame qui contient le mot de passe de l'utilisateur. Exhibez-le.
- 5) Faites vos comparaisons entres les différents services proposés et conclure quant à la sécurité des transmissions de données.