IUT du Limousin
Département Informatique
M2102/2016/TP1/ER/

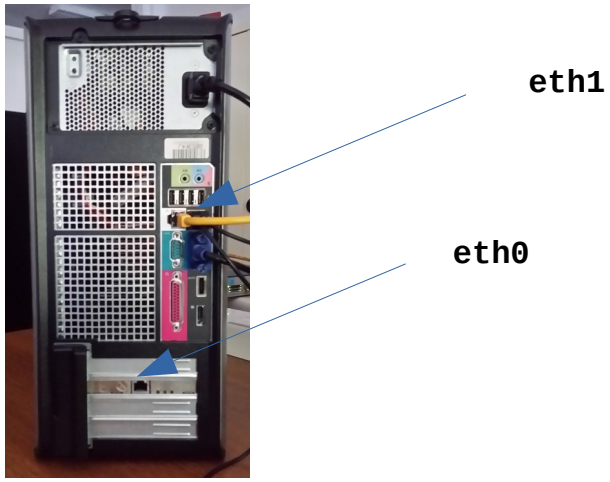
M2012 - TP1

1. Les salles 104 et 105

Les salles 104 et 105, utilisées pour les TP réseaux sont constituées de PC fonctionnant sous Debian7 et incluent une machine virtuelle **Debian7_Réseau** dédiée aux TP de réseau. Comme les autres salles de l'IUT, elles sont installées sur un réseau en /26 :

`164.81.118.0/26`	pour la salle **105**
`164.81.118.64/26`	pour la salle **104**

Les machines comportent toutes 2 cartes réseaux qui apparaissent sous les noms ***eth0*** et ***eth1***. La carte ***eth1*** correspond à la carte réseau de la carte mère (branchée ici avec un câble jaune), c'est celle qui doit être utilisée **sauf mention explicite du contraire**.



Au niveau de l'adressage IP, **les 20 premières adresses sont réservées** (pour les machines physiques), vous devrez donc utiliser pour les VM les adresses **à partir de la 21** pour la salle **105**, et **à partir de la 85** pour la salle **104**, en fonction de votre numéro de machine (**adresse à utiliser = adresse sur le boîtier + 20**) :

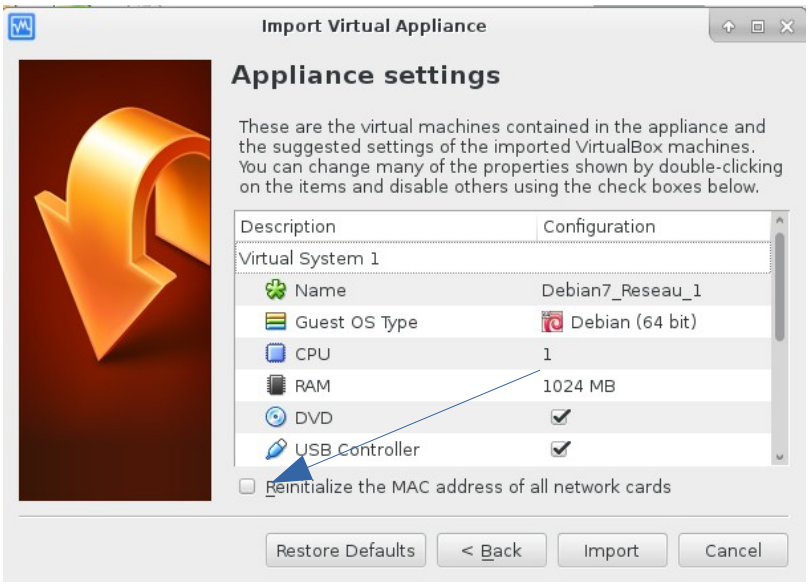
adresse machine physique **`164.81.118.65`** → adresse de VM **`164.81.118.85`**

Afin de compléter la configuration IP, vous aurez besoin des adresses suivantes :

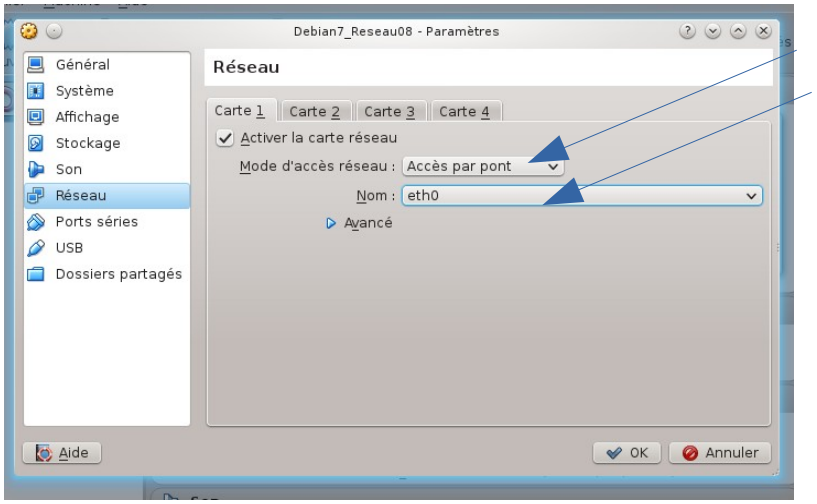
- la passerelle du réseau de la salle **105** : `164.81.118.62`,
- la passerelle du réseau de la salle **104** : `164.81.118.126`,
- les serveurs DNS : `164.81.1.4` et `164.81.1.5`

Import des VM

Pour tous les TP, vous travaillerez sur la VM **Debian7_Réseau** fournie, que vous devrez importer, puis configurer. Au moment de l'importation, il est obligatoire de **réinitialiser les adresses MAC** pour éviter tout conflit :



Il faut ensuite utiliser des paramètres réseau spécifiques, et notamment vérifier que les **2 adaptateurs** réseaux sont en **connexion par pont** vers **eth0** pour le premier et **eth1** pour le second :



Si vous le souhaitez, vous pouvez partager un dossier (par exemple votre dossier ***Perso***) entre la machine physique et la VM, via le menu *Dossiers partagés*, et avec l'option *Montage automatique*. Une fois la VM démarrée, vous trouverez le contenu du répertoire ***Perso*** sous :

```
/media/sf_<nom du partage>
```

CONFIGURATION IP SOUS LINUX

1. Commandes utiles pour le TP

1.1. La commande `ifconfig`

La commande `ifconfig` est utilisée (**en tant que root**) pour configurer les interfaces réseau sous Linux en ligne de commande. Cette commande propose plusieurs options parmi lesquelles on trouve notamment :

- `ifconfig –a`

Cette option va lister l'ensemble des interfaces disponibles sur la machine, qu'elles soient utilisées ou non, activées ou non.

- `ifconfig <nom d'interface> [<up | down>]`

Associée à un nom d'interface, la commande `ifconfig` permet soit de consulter l'état de ladite interface, soit de l'activer/désactiver.

```
# ifconfig eth0          consulte l'état de l'interface eth0
# ifconfig eth1 up       active l'interface eth1
```

- `ifconfig <nom d'interface> <@IP> netmask <mask>`

La commande `ifconfig` peut bien sûr être utilisée pour affecter une adresse IP à une interface donnée. Si on ne précise pas le masque de sous-réseau, celui-ci sera calculé par défaut à partir de la classe de l'adresse. **Il faut donc toujours préciser le masque !**

```
# ifconfig eth0 123.78.43.1/16
# ifconfig eth1 192.168.34.1 netmask 255.255.255.0
```

Remarque: Pour plus d'informations : `man ifconfig`.

1.2. La commande `ping`

La commande `ping` est une des commandes que vous allez le plus utiliser en réseau, elle permet de tester simplement la connectivité entre 2 machines repérées par une adresse IP. Elle peut s'utiliser simplement de la manière suivante :

```
$ ping -c <nombre de messages> <@IP destination>
```

Le principe qui sera vu en détail la semaine prochaine, est d'envoyer un message à la machine destination, laquelle va y répondre, confirmant ainsi la connectivité dans les 2 sens entre les 2 machines.

2. Notion de réseau local

Vous allez commencez en travaillant par rangée, avec 4 machines et 3 ou 4 étudiants par rangée. Chaque rangée choisira son **propre réseau privé de classe C** qui devra être différent de celui des autres rangées.

Numéro du réseau choisi : _____._____._____._____/_____

1. Listez toutes les interfaces réseaux disponibles sur votre machine.

Commande utilisée

Résultat

2. Quel résultat obtenez-vous en utilisant la commande prédédente sans option ? Pourquoi ?

3. Configurez les interfaces **eth1** des 4 machines pour qu'elles appartiennent au réseau choisi en utilisant les numéros suivants pour la partie machine de l'adresse IP :

56 131 189 223

Commande utilisée (pour votre machine)

Utilisez la commande `ping` pour vérifier la connectivité entre les machines de votre réseau :

Connectivité (0/N)	131	189	223
56			
131	[redacted]		
189	[redacted]	[redacted]	

4. Vous allez maintenant mettre en place 2 sous-réseaux au sein de votre réseau de classe C. Pour cela, retapez la même commande `ifconfig` que précédemment (même adresse IP), mais en spécifiant un réseau en **/25**.

Commande utilisée (pour votre machine)

Utilisez la commande `ping` pour vérifier à nouveau la connectivité entre vos machines :

Connectivité (0/N)	131	189	223
56			
131	[redacted]		
189	[redacted]	[redacted]	

Calculez alors les caractéristiques des sous-réseaux pour vérifier que le résultat obtenu est conforme aux principes vus en cours et en TD :

Numéro réseau 1 : _____ / ____

Adresses IP : _____ → _____

Numéro réseau 2 : _____ / ____

Adresses IP : _____ → _____

5. Modifiez à nouveau le masque, afin d'obtenir 4 sous-réseaux, toujours sans changer les IP.

Commande utilisée (pour votre machine)

Utilisez la commande `ping` pour vérifier à nouveau la connectivité entre vos machines :

Connectivité (0/N)	131	189	223
56			
131	[redacted]		
189	[redacted]	[redacted]	

6. On souhaiterait que les 4 machines se retrouvent dans des sous-réseaux différents. Quelle est l'adresse qui pose problème pour ce faire ?

Adresse « erronée » : _____

Par quelles adresses pourrait-elle être remplacée afin d'obtenir le fonctionnement souhaité ?

Effectuez la modification d'adresse, et vérifiez à nouveau la connectivité.

7. Pour cette dernière question, repassez la machine n°56 en **/24**, sans modifier la configuration des autres machines.

Quel résultat obtenez-vous quand vous faites un ping **depuis la machine 56** vers une des autres ?

Quel message obtenez-vous quand vous faites un *ping* depuis une des autres machines **vers la 56** ?

Expliquez pourquoi les comportements sont différents :

FONCTIONNEMENT DU RÉSEAU LOCAL

1. Le logiciel *Wireshark*

1.1. Présentation

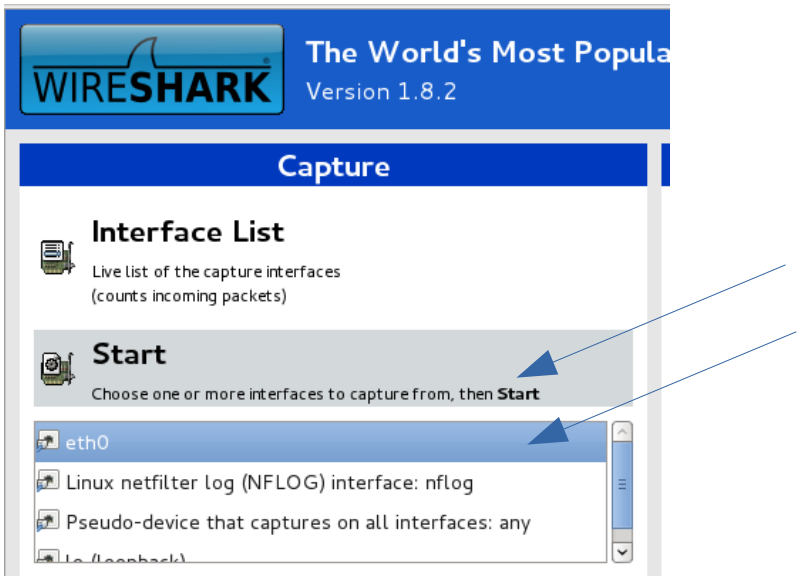
Wireshark est un outil de capture et d'analyse de paquets réseau en ligne. Il fonctionne également en mode hors-ligne pour faire de l'analyse de trames. C'est un logiciel libre et multiplateforme dont les principales caractéristiques sont les suivantes :

- support de plusieurs centaines de protocoles

- filtrage avancé des données, lors de la capture et aussi lors de l'analyse.
- interface graphique pour la navigation dans les données capturées
- compatible avec d'autres formats de capture
- décryption de nombreux protocoles (e.g. IPSec, Kerberos, WPA).

1.2. Utilisation

La capture des trames peut être simplement démarrée via l'écran d'accueil. Pour ce faire, il suffit de choisir l'interface sur laquelle on souhaite capturer les trames et de cliquer sur le bouton *Start* :



Pour arrêter la capture, il suffit d'utiliser le bouton situé dans la barre de menu. On peut alors naviguer de manière simple et intuitive dans les différentes trames capturées. **Pour chacune d'entre elles, *Wireshark* va décrypter l'information en identifiant le type de trame et les informations qu'elle contient.**

2. Étude du trafic

2.1. Notion de réseau local

1. Vous allez utiliser *Wireshark* pour vérifier l'hypothèse formulée à la dernière question de la partie précédente. Pour cela, lancez une capture *Wireshark* sur la machine n°56 et sur une des machines restées en /26.

Utilisez la commande `ping` pour envoyer un message de la machine en /26 vers la machine n°56. Pouvez-vous visualiser sous *Wireshark* une trame correspondant à cette commande ?

2. Utilisez cette fois la commande `ping` sur la machine n°56 pour contacter l'autre machine. Pouvez-vous visualiser sous *Wireshark* une trame correspondant à cette commande :

- sur la machine N° 56 (OUI/NON) : _____
- sur l'autre machine (OUI/NON) : _____

Ces captures confirment-elles votre hypothèse précédente ?

3. Dans quel sens l'envoi de message est-il possible entre ces 2 machines ?

Quelle échange **bidirectionnel** a nécessairement eu lieu, même si vous ne l'avez par observé ?

Pourquoi cet échange a-t-il pu avoir eu lieu alors que le ping ne fonctionne pas ?

2.2. Ping sur le réseau local

1. Vous allez maintenant travailler chacun sur votre machine. Modifiez la configuration IP de votre machine, de manière à utiliser son adresse « habituelle » (IP notée sur le boitier + 20).

Commande utilisée

2. Consultez maintenant le cache ARP de votre machine, à l'aide de la commande suivante :

```
# arp -a
```

Si la table n'est pas vide, videz-là en utilisant la commande suivante pour chacune des lignes présentes :

```
# arp -d <@IP>
```

3. Relancez *Wireshark* , et démarrez une capture de trames en choisissant la bonne interface de capture. Faites alors **un « ping » et un seul** vers la machine de l'enseignant (**164.81.118.61** en salle **105** et **164.81.118.125** en salle **104**), puis arrêtez la capture.

Commande utilisée

4. Analysez tout d'abord les trames ARP échangées, et retrouvez :

- l’adresse IP et l’adresse MAC de votre machine,

  IP : _____ MAC : _____

- l’adresse IP et l’adresse MAC de limds1,

  IP : _____ MAC : _____

5. Vérifiez que suite à cet échange, l'adresse MAC de limds1 a été enregistrée par votre machine.

Commande utilisée

Adresse MAC enregistrée : OUI / NON

6. Etudiez maintenant les trames correspondant au « ping » et relevez :

- le nom du protocole utilisé par la commande `ping` : _____
- le(s) protocole(s) dans le(s)quel(s) il est encapsulé (pile de protocoles) :

- la destination de la commande ping :

dst IP : _____ dst MAC : _____

A qui appartient cette adresse MAC ? Pourquoi ?

2.3. Ping hors du réseau local

1. Déclarez maintenant une passerelle de sortie du réseau local (ceci sera vu lors du TD2):

```
# route add default gw 164.81.118.62     en salle 105
# route add default gw 164.81.118.126    en salle 104
```

2. Consultez maintenant le cache ARP de votre machine, et videz-le si nécessaire. Relancez une capture sous *Wireshark* , et envoyez **un « ping » et un seul** vers la machine d'adresse IP 8.8.8.8, puis arrêtez la capture.

3. Analysez tout d'abord les trames ARP échangées, et retrouvez :

- l'adresse IP et l'adresse MAC de la machine « cible »

  IP : MAC :

Qui est cette machine ? Pourquoi ?

4. Étudiez maintenant les trames correspondant au « ping » et relevez la destination de la commande ping :

- l'adresse IP destination et la machine correspondante :

  @IP : _____ machine : _____

- l'adresse MAC destination et la machine correspondante :

  @MAC : _____ machine : _____

5. Pouvez-vous connaître l'adresse MAC de la machine destination, c'est à dire celle de 8.8.8.8 ?

LE TP EST TERMINE, SUPPRIMEZ LA VM,

ET ÉTEIGNEZ LA MACHINE
