



ETUDE D'UNE TRAME TCP

Sommaire

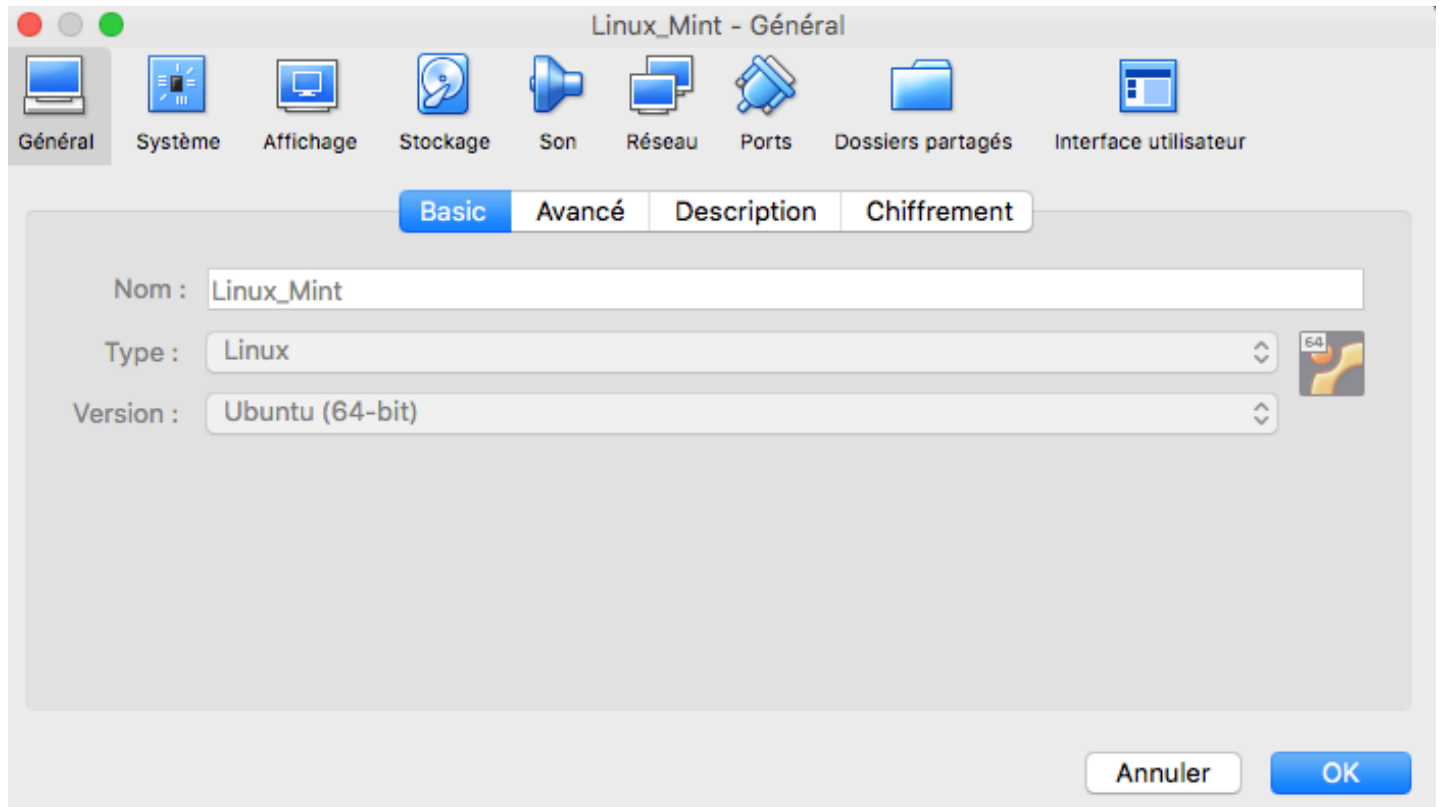
- 1. Introduction..... 3
- 2. Les modes réseaux 3
- 3. Travail demandé 4
- 4. Réseau avec pont (bridge) 5
- 5. Caractéristiques de notre connexion 5
- 6. Analyse de transfert de données..... 7
 - 6.1 Mise en œuvre du script..... 7
 - 6.2 Analyse des résultats 7

1. Introduction

Oracle VM Virtual box permet d'exécuter plusieurs systèmes d'exploitation sur une même machine simultanément et sans passer par un « dual boot ».

Cette technique prend tout son sens en phase de test de développement multiplateforme Linux, Windows, ...

En ce qui concerne la gestion des réseaux, VirtualBox fournit jusqu'à 8 cartes réseaux par machine virtuelle.



2. Les modes réseaux

Les principaux modes proposés par VBox sont :

- **Réseau interne** : On peut l'utiliser pour créer un type différent de réseau sur une base logicielle, visible pour les machines sélectionnées, mais pas pour les applications de l'hôte ou du monde extérieur.
- **Réseau privé hôte (Host-only)** : On peut l'utiliser pour créer un réseau contenant l'hôte et un ensemble de machines virtuelles, sans avoir besoin de l'interface réseau physique de l'hôte. À la place, une interface réseau virtuelle est créée sur l'hôte, offrant une connectivité entre les machines virtuelles et l'hôte.
- **Réseau avec pont (bridge)** : Lorsque vous l'activez, VirtualBox se connecte à une de vos cartes réseaux installées et il échange des paquets réseaux directement, dépassant la pile réseau du système d'exploitation de votre hôte. En résumé votre système invité est accessible "directement" à partir de votre réseau physique comme s'il était connecté physiquement à l'interface réseau en utilisant un câble réseau : l'hôte peut envoyer des données à l'invité via cette interface et en recevoir. Cela veut dire que vous pouvez régler du routage ou des ponts entre l'invité et le reste de votre réseau.
- **Network Address Translation (NAT)** : Une machine virtuelle dont NAT est activé agit exactement comme un vrai ordinateur qui se connecte à Internet par un routeur. Le "routeur", dans ce cas, est le moteur réseau de VirtualBox, qui dirige le trafic depuis et vers la machine virtuelle de façon transparente. Dans VirtualBox, ce routeur se place entre chaque machine virtuelle et l'hôte. Cette séparation maximise la sécurité puisque, par défaut, les machines virtuelles ne peuvent pas se parler.

C'est cette fonction de NAT qui est normalement assurée par votre box sur votre réseau perso (sauf si un autre routeur assure cette fonction). L'inconvénient principal est que dans ce cas, la machine virtuelle est invisible et injoignable depuis le réseau extérieur sauf si vous réglez une redirection de ports.

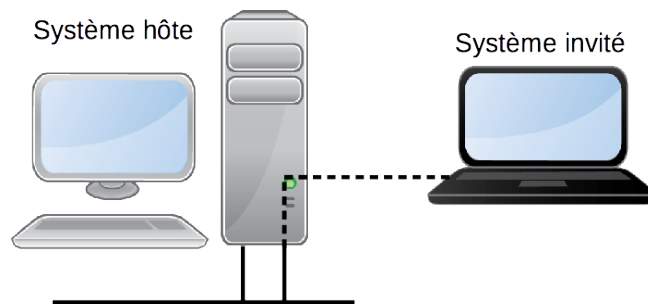
En consultant le manuel de l'utilisateur du logiciel, vous pouvez trouver toutes les informations concernant les différentes configurations : https://www.virtualbox.org/download/testcase/manual/UserManual_fr_FR.pdf

3. Travail demandé

En vous basant sur le descriptif précédent, choisissez le mode réseau à configurer afin de permettre à notre machine virtuelle de se connecter sur le réseau du lycée comme une machine physique

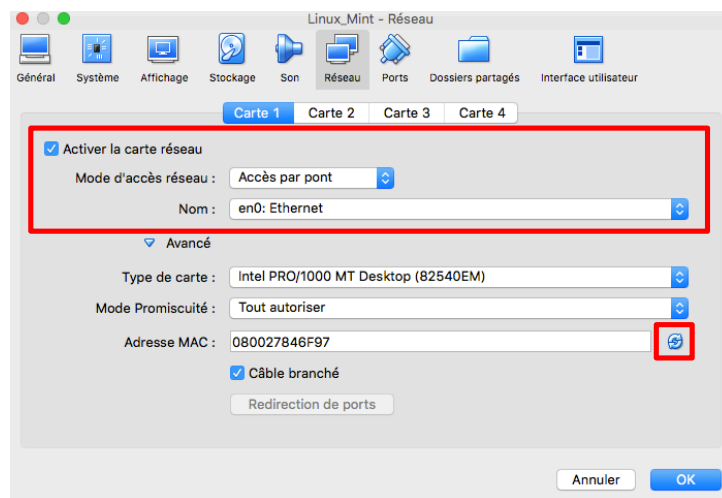
4. Réseau avec pont (bridge)

Ce mode permet à VirtualBox d'intercepter les données du réseau physique et d'y envoyer des données, ce qui crée de fait une nouvelle interface réseau logicielle. Quand un invité utilise une telle interface, cela se passe, sur le système hôte, comme si l'invité était connecté physiquement à l'interface réseau en utilisant un câble réseau.



- Ouvrir le logiciel VirtualBOX si ce n'est pas déjà fait.

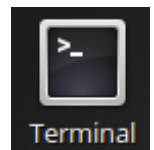
Pour passer l'interface réseau d'une machine virtuelle en mode "Accès par pont", allez sur l'onglet "Réseau" de la boîte de dialogue des paramètres de la machine virtuelle dans l'interface graphique et sélectionnez :



A ce stade, on peut modifier l'adresse physique MAC du poste invité. A faire en cas d'adresse IP double sur le réseau (à tester en live dans la salle...).

Cliquer le nombre de fois nécessaire afin que chaque machine puisse avoir une adresse IP différente sur le réseau. Voir avec le prof qui vous donne les informations (TP encore en Bêta- test...)

5. Caractéristiques de notre connexion



Après avoir démarré la machine virtuelle, démarrer une fenêtre « Terminal » (sur le bureau).

- Tapez la commande : **\$ ifconfig (ipconfig sous windows)**

```
chaplin@chaplin-VirtualBox ~
Fichier Édition Affichage Rechercher Terminal Aide
chaplin@chaplin-VirtualBox ~ $ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:84:6f:97
        inet adr:192.168.0.12  Bcast:192.168.0.255  Masque:255.255.255.0
```

Vous devriez obtenir une IP du type : 172.16.X.X conforme au plan d'adressage du lycée.

Afin de connaître la passerelle du réseau c'est-à-dire le poste qui permet de sortir du réseau local vers Internet, on peut taper la commande suivante dans le terminal :

\$ route -n

Vous pouvez vérifier que le réseau est pleinement accessible en vérifiant que votre VM accède à la passerelle du réseau : **ping 172.16.0.252**

- En examinant les résultats de la commande examiner les informations relatives à votre connexion réseau :

Link encap : **HWaddr :** **Inet adr :**
Bcast : **Masque :**

Pour les questions suivantes vous consulterez les pages 6 à 8 du doc ressource.

- Déterminer la signification de ces informations ainsi que leur fonction dans la jonction au réseau.

Lors de la définition du protocole d'adressage IP, certaines adresses ont été réservées pour un usage en réseau privé pour les différentes classes :

Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255

Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255

Les adresses privées de la classe C : 192.168.1.0 à 192.168.255.255

- A l'aide de toutes les informations précédentes, déterminer la classe du réseau du lycée et le nombre de machines qui pourraient être connectées au réseau.

Afin de connaître l'adresse IP de notre machine en naviguant sur Internet, consulter le site :

<http://www.whatismyip.com/>

- Noter cette adresse et la comparer avec celle de la machine voisine. Que remarquez-vous ?

De retour sur notre terminal Linux, nous allons essayer d'en savoir un peu plus sur cette adresse. Saisir la commande suivante :

\$ host 194.199.75.45

Noter les informations obtenues :

Puis : **\$ whois 194.199.75.45**

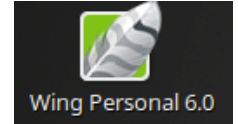
- A quel réseau appartient cette adresse ?
- Quelle est la classe de ce réseau ? Combien de machines sont-elles adressables sur ce réseau ?
- Qui est le FAI ?

6. Analyse de transfert de données

Afin d'analyser comment se passe le transfert de données entre 2 machines, nous allons mettre en œuvre plusieurs logiciels :



- **Wireshark** : un « sniffeur » de connexion qui permet d'examiner les trames qui circulent sur un réseau.
- **Wing** : un IDE Python avec lequel nous allons lancer un script permettant de créer une connexion Client / Serveur.




6.1 Mise en œuvre du script

- Travailler en binôme avec votre machine voisine.
- Lancer le logiciel Wireshark et sélectionner la connexion réseau active **enp0S3 (??)**
(si besoin arrêter la capture en appuyant sur l'icône rouge)
- Lancer le logiciel Wing et ouvrir si ce n'est pas fait le script « **transfert-fichier-v2.7.py** »
- Exécuter le script sur une machine en serveur (sans saisir de nom de fichier) et l'autre machine en client.
Saisir le nom du fichier à transférer : **coming back to life.flac**

Le serveur est en attente d'une connexion alors :

- Saisir sur le client, l'IP de la machine serveur puis valider.

Le serveur demande confirmation de la réception du fichier. NE PAS REPONDRE POUR L'INSTANT !!

- Passer dans Wireshark et commencer la « reniflage » du réseau en cliquant sur .
- Repassez sur Wing Python, et répondre « o » sur la machine serveur. Le transfert commence...
- A la fin du transfert, stopper la capture WireShark.

6.2 Analyse des résultats

Sur WireShark, vous devez voir un amas d'informations illisibles... c'est normal, il va falloir faire un peu de ménage :

- Etant donné que l'on ne veut examiner que les trames entre nos 2 machines Client / serveur, on va choisir les trames correspondantes à cette connexion :



Dans la barre tout en haut de la fenêtre, saisir la commande suivante :

lpp.addr==... suivi de l'adresse de la machine voisine puis valider.

Vous devriez y voir plus clair.

No.	Time	Source	Destination	Protocol	Length	Info
13	7.90208933	192.168.0.20	192.168.0.12	TCP	66	2110 → 39240 [PSH, ACK] Seq=1 Ack=3 Win=229 Len=0 TSval=1082946375 TSecr=274553856
14	7.903032936	192.168.0.12	192.168.0.26	TCP	66	39240 → 2110 [ACK] Seq=1 Ack=3 Win=229 Len=0 TSval=274553856 TSecr=1082946375
15	7.906081831	192.168.0.12	192.168.0.26	TCP	1090	39240 → 2110 [PSH, ACK] Seq=1 Ack=3 Win=229 Len=1024 TSval=274553856 TSecr=1082946375
16	7.906402091	192.168.0.26	192.168.0.12	TCP	66	2110 → 39240 [ACK] Seq=3 Ack=1025 Win=4084 Len=0 TSval=1082946378 TSecr=274553856
17	7.910782558	192.168.0.12	192.168.0.26	TCP	1090	39240 → 2110 [PSH, ACK] Seq=1025 Ack=3 Win=229 Len=1024 TSval=274553858 TSecr=1082946378
18	7.911029881	192.168.0.26	192.168.0.12	TCP	66	2110 → 39240 [ACK] Seq=3 Ack=2049 Win=4064 Len=0 TSval=1082946382 TSecr=274553858
19	7.911046087	192.168.0.12	192.168.0.26	TCP	1090	39240 → 2110 [PSH, ACK] Seq=2049 Ack=3 Win=229 Len=1024 TSval=274553858 TSecr=1082946382

▶ Frame 15: 1090 bytes on wire (8720 bits), 1090 bytes captured (8720 bits) on interface 0
 ▶ Ethernet II, Src: PcsCompu 84:6f:97 (08:00:27:84:6f:97), Dst: Apple_95:89:50 (60:c5:47:95:89:50)
 ▶ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 192.168.0.26
 ▶ Transmission Control Protocol, Src Port: 39240, Dst Port: 2110, Seq: 1, Ack: 3, Len: 1024
 ▶ Data (1024 bytes)

Cadre1, on peut voir les trames transmises

Cadre 2, les informations couche par couche relatives à la trame sélectionnée cadre 1

0000	60	c5	47	95	89	50	08	00	27	84	6f	97	08	00	45	00	...	G..P..'.o..E.
0010	04	34	9a	6c	40	00	40	06	1a	e1	c0	a8	00	0c	c0	a84.l0.0.
0020	00	1a	99	48	08	3e	9a	d8	97	1c	a2	43	bc	1c	80	18H>...C... ..
0030	00	e5	85	9d	00	00	01	01	08	0a	18	5d	5c	00	40	0c]\0.
0040	73	47	66	4c	61	43	00	00	00	22	19	00	19	00	00	23	...	s0FLAC..".#
0050	62	00	49	60	17	70	03	70	02	30	7c	60	40	bc	e1	e5	...	b.l'.p.p.'0]0...
0060	00	e1	f9	20	c7	e9	bd	d9	e1	ab	f2	51	04	00	01	19Q...
0070	20	00	00	00	72	65	66	65	72	65	6e	63	65	20	6c	69refe rence li
0080	62	46	4c	41	43	20	31	2e	32	2e	31	20	32	30	30	37	...	bFLAC 1. 2.1 2007
0090	30	39	31	37	00	00	00	00	25	00	00	00	57	41	56	45	...	0917....%.WAVE
00a0	46	4f	52	4d	41	54	45	58	54	45	4e	53	49	42	4c	45	...	FORMATX TENSIBLE
00b0	5f	43	48	41	4e	4e	45	4c	5f	4d	41	53	4b	30	30	58	...	_CHANNEL_MASK=0X
00c0	33	0d	00	00	00	56	41	4c	49	44	5f	42	49	54	53	3d	...	3....VAL ID BITS=
00d0	32	34	06	00	00	00	48	44	43	44	3d	30	11	00	00	00	...	24....HD CD=0....
00e0	41	52	54	49	53	54	3d	50	69	6e	6b	20	46	6c	6f	79	...	ARTIST=P ink Floy
00f0	64	19	00	00	00	54	49	54	4c	45	3d	43	6f	6d	69	6e	...	d...TIT LE=Comin
0100	67	20	42	61	63	60	20	54	6f	20	4c	69	66	65	0e	00	...	g Back T o Life...
0110	00	00	54	52	41	43	40	4e	55	4d	42	45	52	30	30	38TRACKN UMBER=00
0120	17	00	00	00	41	4c	42	55	4d	20	41	52	54	49	53	54ALBU M ARTIST
0130	3d	50	69	6e	6b	20	46	6c	6f	79	64	17	00	00	00	41	...	=Pink Fl oyd...A
0140	4c	42	55	4d	3d	54	68	65	20	44	69	76	69	73	69	6f	...	LBUM=The Divisio
0150	6e	20	42	65	6c	6c	09	00	00	00	44	41	54	45	3d	31	...	n Bell...DATE=1
0160	39	39	34	10	00	00	00	47	45	4e	52	45	3d	50	72	6f	...	994...G ENRE=Pro
0170	67	72	65	73	73	69	76	65	20	52	6f	63	6b	00	00	00	...	gressive Rock...
0180	00	43	4f	4d	4d	45	4e	54	3d	06	01	09	b1	00	00	00COMMENT =.....
0190	03	00	00	00	0a	69	6d	61	67	65	2f	6a	70	65	67	00ima ge/jpeg.
01a0	00	00	00	00	00	02	58	00	00	02	ff	00	00	00	18	00X.
01b0	00	00	00	00	01	09	87	ff	d8	ff	e0	00	10	4a	46	49JFI
01c0	46	00	01	01	01	00	69	00	60	00	00	ff	db	00	43	00	...	F.....C.
01d0	07	05	05	06	05	04	07	06	05	06	08	07	07	08	0a	11
01e0	00	0a	09	09	0a	15	0f	10	0c	11	18	15	1a	19	18	15
01f0	18	17	1b	1e	27	21	1b	1d	25	1d	17	18	22	2e	22	25!'.%.%.%"
0200	28	29	2b	2c	2b	1a	20	2f	33	2f	2a	32	27	2a	2b	2a	...	()+ + / 3/*2'+*
0210	ff	db	00	43	01	07	08	08	0a	09	0a	14	0b	0b	14	2aC.....*

Cadre 3, les informations brutes (le « dump ») relatives à la couche sélectionnée cadre 2 en Hexadécimal

Examinons d'un peu plus près ce qu'il se passe :

- Sélectionner une trame dont le contenu ressemble un peu à la capture d'écran et relever les informations suivantes :
 - Cadre 2 : port de transmission du protocole TCP :
 - Cadre 2 : Longueur de la trame TCP (Len) :
 - Cadre 3 : Groupe mythique, auteur de la chanson transmise :
- Retourner sur l'IDE Python et examiner le script pour retrouver le port de connexion et la longueur de la trame.

Voilà on arrêtera là pour l'examen des trames car on pourrait y passer des heures... Dans le prochain travail, on va voir comment ouvrir une connexion entre 2 machines en Python.