TP 1 – Initiation aux réseaux

Objectif

Ce TP a pour objectif de manipuler les utilitaires de base utilisés dans l'univers des réseaux.

Vous utiliserez lors de ce TP le système d'exploitation linux (OpenSuse).

Astuce à connaitre : LA COMMANDE NE MARCHE PAS, POURQUOI ?

Si vous n'arrivez pas à trouver où se trouve une commande. Taper la commande **whereis** (comme ci-dessous) ou la commande **locate**

whereis nomDeLaCommandeATrouver

Par exemple

$ whereis traceroute

/usr/sbin/traceroute

En tapant la commande **whereis ifconfig**, nous nous apercevons que la commande **traceroute** se trouve dans le répertoire /usr/sbin

Il suffit donc pour exécuter cette commande de taper /usr/sbin/traceroute

$ /usr/sbin/traceroute

Une alternative consiste à se placer dans le répertoire /usr/sbin et à taper la commande ./traceroute comme ci-dessous.

$ cd /usr/sbin

$ ./traceroute

Vous aurez de grande chance que les commandes auquel vous souhaitez avoir accès se trouvent dans les répertoires suivants :

/sbin

/bin

/usr/sbin
/usr/bin

Deuxième astuce : JE NE SAIS PAS CE QUE FAIT CETTE COMMANDE OU COMMENT JE REPOND A VOTRE QUESTION

La commande man vous permet d'avoir accès aux informations concernant une commande. Par exemple, en tapant la commande vous apprendrez à quoi sert cette commande et quelles sont les options offertes par cette commande

$ man traceroute

Une alternative consiste aussi à taper la commande

$ traceroute -h

Troisième astuce : JE N'ARRIVE PAS A ME PLACER DANS LE BON REPERTOIRE…

En appuyant sur la touche tab, vous verrez que les lignes se compléteront

1) Adressage, routes statiques

Démarrer une invite de commande, tapez les commandes demandées ci-dessous et répondez aux questions qui suivent.
La commande **`ip`** vous permet de configurer et d'accéder à des informations concernant les interfaces réseaux de votre ordinateur et les tables de routage. La commande **`route`** vous permet de manipuler vos tables de routage.

Question 1
Taper la commande : **`ip addr show`**
Taper la commande : **`ip route show`**

Question 2
Tapez la commande **`route -n`** (ou **`routel`** sur certains systèmes Linux).

Recopier, examiner et expliquer le résultat. Etant donné que les réponses renvoyées par des commandes windows et unix peuvent différer, certaines questions peuvent ne pas s'appliquer à votre environnement.

Question 3
Par ailleurs, vous déterminerez :
Quelle est votre adresse MAC ?
Quelle est votre adresse IP ?
Quelle est le masque de votre réseau ?
Quelle est l'adresse de broadcast de votre réseau ?
Quelle est l'adresse de la passerelle ?

Question 4
Tapez la commande **`ifconfig`** et comparez les informations fournies par cette commande par rapport à celles données par la commande **`ip addr show`**.

Question 5
Déterminer à quoi servent les commandes suivantes :

- **ip addr add 192.168.50.5 dev em1**
- **ip addr del 10.0.3.1/24 dev em1**
- **ip route add 10.10.3.1/24 via dev lxcbr1**
- **ip route add default gw 192.168.1.254 em1**
- **ip route add 10.1.30.0/24 via 192.168.10.30 dev lxbr1**

Question 6
La commande **`ping`** permet d'envoyer un paquet à une machine ayant une adresse donnée.
Taper **`ping`** *votre_adresse_ip*
Tester la commande **`ping`** avec l'adresse

- 127.0.0.1,
- avec votre adresse,
- du poste d'un de vos voisins (si ce poste est accessible dans votre environnement),
- de la passerelle,
- 195.167.227.250,
- 163.173.128.6,

Comment expliquez-vous vos résultats ?

Question 7
En utilisant la commande **`ping`**, faites un broadcast à toutes les machines de votre (sous)-réseau.
Quelle est la commande que vous avez utilisée ?

La commande **cat** vous permet d'afficher le contenu d'un fichier.

Taper la commande suivante :
cat /etc/services

Le fichier /etc/services vous permet de savoir quels sont les ports TCP et UDP ouverts sur votre machine. Pour information, les ports qui ont une valeur inférieur à < 1024 sont des ports utilisés par des protocoles connus et normalisés via l'IETF dont la liste est maintenue par IANA (The Internet Assigned Numbers Authority). Les ports allant de 1024 à 49151 sont des ports assignés par IANA utilisables par l'utilisateur et les ports allant de 49152 à 65535 sont des ports non assignés.
Vous pouvez la consulter à partir de :
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Question 8
Quel est le port utilisé par le protocole HTTP ? Ce port est il ouvert sur votre machine ?

Chaque carte réseau Ethernet possède une adresse MAC unique. La commande **`arp`** affiche et modifie les entrées du cache ARP (Address Resolution Protocol), qui contient une table permettant de stocker temporairement les correspondances entre adresses IP et adresses MAC.
Utilisée sans paramètres, la commande **`arp`** affiche de l'aide.

Question 9
Taper la commande suivante qui vous permet d'afficher les informations contenues dans votre cache arp :
`arp -a`
L'adresse **`ff:ff:ff:ff:ff:ff`** correspond à quoi ?

Question 10
Faite un **`ping`** sur l'adresse d'une machine qui n'est pas dans le cache.
Retaper la commande **`arp -a`**, que se passe-t-il ?

L'utilitaire **`wireshark`** vous permet de surveiller ce qu'il se passe sur votre réseau. Démarrer votre utilitaire et surveillez l'interface **em1**. Vous allez capturer les messages **`arp`** émis.

Question 11
Il vous faut déterminer le format des échanges suivants (il vous faut retaper les dernières commandes).
Dessiner une trame ARP et expliciter ce qui est échangé au niveau de la couche 2 et 3.

2) Routage

La commande **`traceroute`** permet d'afficher une route empruntée par le trafic IP entre 2 machines.

Question 12
Taper : (sous linux) la commande **`traceroute www.cnam.fr`**
puis **`traceroute www.yahoo.fr`**

Que constatez-vous ?

Question 13
Aller sur le site www.traceroute.org . Essayer de tracer des routes depuis divers endroits de la planète et regardez pour quelles zones géographiques le nombre de sauts est le plus petit et le plus grand.

3) Nommage

Le fichier **/etc/resolv.conf** précise des informations relatives aux serveurs DNS.
Quel est le (ou les) serveurs DNS dont dispose votre machine ?

Question 14

Aller sur le site www.gandi.net qui est un « *registrar* » permettant d'enregistrer des noms de domaine .com .net .org .biz .info :

- Chercher si votre nom de famille est disponible en .com
- Chercher grâce à la rubrique "**whois**" du menu "**Nom de domaine**" qui a enregistré le nom de domaine **france5.com**
- Chercher grâce à la rubrique "**whois**" du menu "**Nom de domaine**" qui a enregistré le nom de domaine **cnam.fr,** décrivez qu'elle est l'entité (registrar) du cnam.

Question 15

Aller sur le site de l'AFNIC www.afnic.fr. Vérifier si votre nom de famille est disponible en .fr.
Chercher qui a enregistré le nom de domaine **france5.fr**

La commande **`nslookup`** permet d'obtenir la mise en correspondance entre l'adresse IP et le nom d'une machine. Elle permet de questionner les serveurs de noms (DNS). Si cette commande ne marche pas, vous pouvez utiliser l'adresse : http://www.kloth.net/services/nslookup.php

Question 16

Taper la commande **`nslookup`**.
Quand vous obtenez le prompt **>** taper **www.yahoo.fr**, puis taper sur la touche <Entrer>. *Qu'obtenez-vous ? Donnez la signification des champs que vous obtenez.*

Question 17

Taper **195.167.227.249.** *Qu'obtenez-vous ?*

Question 18

Pour chercher quels sont les serveurs DNS qui gèrent un nom de domaine, taper la commande
set type=NS
taper **cnam.fr** pour connaître les serveurs de nom qui gère le nom de domaine du cnam.

Question 19

Pour chercher quels sont les serveurs de messagerie qui gèrent le courrier de *gmail.com* taper la commande
`set type=MX` (MX = mail exchanger)
puis taper : **`gmail.com`**

Question 20

taper **`cnam.fr`** pour connaître les serveurs de messagerie qui gère son courrier, *qu'obtenez vous?*
taper **`exit`** pour sortir

4) Connexions

La commande **`netstat`** permet d'obtenir la liste des connexions établies par votre machine au cours des dernières minutes.

Question 21

Taper **`netstat -i`**, *qu'obtenez vous, à quoi sert cette commande ?*

Question 22

Taper **`netstat -r`** , *qu'obtenez vous, à quoi sert cette commande ?*

Question 23

Taper **`netstat -anp`**, *qu'obtenez vous, à quoi sert cette commande ?*

5) Transférer des fichiers et se loger sur une machine

Le protocole FTP est utilisé pour transférer des fichiers d'une machine à une autre. Son utilisation

est peu indiquée car FTP ne chiffre pas la communication. Il existe une alternative pour transférer les fichiers qui est la commande **scp** (*Secure Copy*) qui utilise pour transférer les fichiers un chiffrement qui protège à la fois le *login*, le *mot de passe* et le *fichier*. Cette commande ouvre un tunnel de communication réseau **ssh** (*Secure Shell*) entre deux machines qui chiffré pour transférer les informations. La commande ssh vous permet de vous connecter à une machine distante et d'ouvrir une session shell pour entrer des commandes comme si vous étiez sur la machine sur laquelle vous vous êtes connecté. **scp** est très simple à utiliser, dans un premier temps vous allez créer un fichier pour cela vous pouvez utiliser la commande **touch** qui vous permet de créer un fichier vide :

```
$ touch monfichier
```

Pour transférer le fichier que vous avez créé à votre voisin, récupérez l'adresse IP de votre voisin. Vous utiliserez le nom d'utilisateur que vous avez utilisé pour vous connecter sur la machine (ou demandez en un au professeur).

Question 24

Tapez la commande suivante :

```
$ scp monfichier nom_utilisateur@adresseIPVoisin:nomdufichierdedestination
```

Pour vérifier que le fichier a bien été transféré chez votre voisin, vous allez vous connecter à distance à la machine de votre voisin :

```
$ ssh nom_utilisateur@adresseIPVoisin
```

6) Parler avec un serveur http

Vous allez discuter comme le fait un client avec un serveur http. Http est un protocole de niveau application, sans état (il ne garde aucune mémoire des précédents échanges). Il suit le modèle de type client/serveur : le client émet une requête à laquelle répond le serveur HTTP. Pour obtenir des informations liées à une URL, vous devez émettre une requête de type get.

Question 25

Vous utiliserez **wireshark** de façon à déterminer sur quel protocole se base HTTP. Pour vous connecter sur le port 80 du serveur Web cedric.cnam.fr, vous allez utiliser la commande **telnet** comme suit : **$ telnet cedric.cnam.fr 80**

Une connexion est établie entre le client et le serveur de façon à acheminer la requête et la réponse.

Puis vous allez taper les deux lignes suivantes PUIS ENTRER A LA LIGNE (TAPER SUR ENTER) :

GET / HTTP/1.1
host: cedric.cnam.fr

Expliquez le résultat que vous obtenez.