Module ITC38 Introduction aux réseaux
InfoTronique 3A

Avril 2016

TP 1 : Installation et découverte

Enseignants : Benoît Darties, Mickael Choisnard

Au terme de toutes les séances de TP, chaque groupe devra rendre à son encadrant un compte rendu répondant aux différentes questions et retraçant les différentes manipulations décrites dans les différents énoncés. Ce compte rendu devra être aussi soigné que possible. Les modalités de remise du compte rendu vous seront communiquées par votre encadrant.

Chaque groupe de TP dispose :

- d'un disque dur externe, qui sera le même pour la durée des 5 TPs
- d'une clé Live USB Linux
- d'au moins deux ordinateurs (il est conseillé de garder les mêmes ordinateurs pour les 5 séances)

I. Installation et prise en main :

note avant utilisation : les clés Live USB ont un compte utilisateur par défaut dont le mot de passe est live (le nom d'utilisateur doit être user). Le serveur ssh est activé mais nécessite une modification du fichier /etc/sshd.conf et d'un redémarrage pour fonctionner correctement. Ce point n'est pas essentiel pour l'instant

1. Installation du système

Pour les 5 séances, nous aurons besoin des droits administrateurs sur Linux. Nous utiliserons donc conjointement une clé Live USB Linux, mais également un disque dur externe afin de pouvoir sauvegarder les modifications de la configuration. Dans un premier temps, nous allons installer Linux sur le disque dur externe.

Insérez la clé USB puis démarrez l'ordinateur, et bootez sur la clé USB (en appuyant sur la touche F9, F12 ou touche correspondante selon votre ordinateur). Connectez ensuite le disque dur externe à l'ordinateur, et réalisez l'installation de Linux sur le disque dur externe. Suivez les différentes étapes de l'installation, faites notamment attention au disque de destination, et veillez à installer le chargeur de démarrage sur ce même disque (appel du professeur au besoin). Notez bien le nom d'utilisateur et le mot de passe que vous avez saisi lors de l'installation.

2. Découverte du système

droits administrateurs

Retirez le CD ou la clé USB, et démarrez le système à partir du disque dur USB (au démarrage, touche F12 ou F9 généralement, choix du boot via USB) et authentifiez-vous. Vous disposez des droits administrateurs sur ce système. Ces derniers ne doivent être utilisés que lorsque la situation s'y prête, notamment pour :

- La création et modification de fichiers de configuration système;
- le changement des paramètres réseau bas niveau;
- les programmes nécessitant des droits privilégiés.

Lorsque vous tentez d'écrire sur un fichier dans lequel vous ne disposez pas des droits suffisants ou que vous essayez de lancer en tant que simple utilisateur un programme qui requiert des droits administrateurs , vous aurez un message d'erreur (permission non accordée, accès refusé, droits insuffisants...)

pour exécuter une commande dans la console avec les droits administrateur, on précèdera cette dernière par la commande `sudo`. Par mesure de sécurité, l'utilisation de `sudo` requiert de renseigner périodiquement son mot de passe Par exemple pour éditer le fichier `/etc/group` avec l'éditeur `nano`, on utiliserait la commande suivante :

```
$ sudo nano /etc/group
```

De même, pour lancer un terminal avec les droits administrateur (utilisateur `root`), on ouvrira un terminal et on utilisera l'une des commandes suivantes. Le terminal aura alors les droits `root`. Notons qu'il existe des différences au niveau de l'environnement selon la commande utilisée :

```
$ sudo su
$ sudo -i
$ sudo -s
```

Gestionnaire de packages

Le gestionnaire de packages permet d'installer des outils complémentaires sur le système. Il peut être appelé dans sa version graphique, ou dans sa version console. En mode console, la recherche d'un package à partir de son nom ou d'un mot clé se fait avec la commande suivante :

```
apt-cache search mot-clé
```

L'installation d'un paquet requiert les droits administrateurs et s'effectue avec la commande suivante :

```
sudo apt-get install nom-paquet
```

Cette installation peut également se faire avec les outils graphiques présents dans la distribution de linux

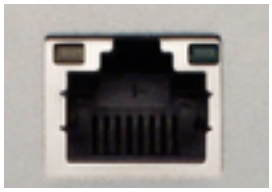
3. Installation des outils nécessaires

1. A l'aide des outils précédemment présentés, Installez les outils suivants qui seront utilisés tout au long des séances de TP, si ces derniers n'étaient pas déjà présents :
   `wireshark` `ethtool` `iperf` `openssh-server`

II. Découverte de l'environnement réseau

1. L'interface réseau

La carte réseau est l'élément physique principal de la communication. Une machine peut disposer de plusieurs cartes (ethernet, wifi, bluetooth ...) possédant différentes caractéristiques. A l'aide de la figure ci-contre identifiez dans un premier temps le nombre de ports ethernet présents sur chacun des postes de travail. Notez particulièrement pour chaque port la présence d'une (parfois deux) diodes associées à la carte. Ces diodes clignotent généralement en cas de transfert de données, et sont très utiles pour déterminer si les connexions sont correctement réalisées.



1. un port ethernet

Chaque élément physique de communication d'une machine (carte ethernet, carte wifi ...) est généralement associé à une (parfois plusieurs) interface logique. Le nom logique d'une interface ethernet est généralement de la forme `eth`***x***, où ***x*** prend une valeur arbitraire. La commande `ifconfig` est une commande essentielle qui vous permet d'afficher la liste des interfaces ainsi que les caractéristiques qui leur sont associées, mais également de modifier certains éléments essentiels associés à ces dernières.

1. Exécutez les commandes suivantes et notez leur résultat :

```
$ ifconfig
$ ifconfig eth0
```

2. Pour chacun des ports ethernet, identifiez et notez le nom de l'interface logique associée, son adresse MAC, son adresse IP si cette dernière en possède une ainsi que son masque réseau (déduisez-en alors le réseau correspondant), et son statut.
3. Utilisez la commande `ethtool` pour déterminer la vitesse de transfert de chaque interface
4. Quelle interface correspond à la carte réseau connectée au commutateur de la salle de TP ? A partir de l'adresse IP et du masque réseau associé, déterminez le nom du réseau associé à cette interface. Vérifiez que ce réseau est bien le même que celui des autres groupes.
5. Consulter les pages du manuel de la commande `ifconfig`, et réalisez les opérations suivante sur l'interface connectée au commutateur :

- Changement de l'adresse IP en une adresse de votre choix
- Changement de l'adresse MAC en une adresse de votre choix
- Désactivation de l'interface
- Restauration de l'adresse MAC originale
- Réactivation de l'interface

Si l'adresse IP originelle n'est pas réaffectée à l'interface, taper la commande suivante (en remplaçant le x de ethx par le numéro de l'interface adéquat):

```
$ sudo dhclient ethx
```

2. Etat du réseau et connexions actives

La commande `ping` permet de «pinger» une machine, c'est à dire de lui demander si elle est active et reçoit bien les paquets qu'on lui envoie. Si l'hôte est actif, il répond en général en renvoyant le paquet envoyé. Le temps de transfert entre l'envoi du paquet et la réception du message est affiché à l'écran. Notons cependant qu'un hôte peut avoir désactivé la fonction de réponse, mais être quand même actif. D'apparence toute simple, la commande `ping` dispose d'une multitude d'options permettant de faire varier de nombreux paramètres, que nous réutiliserons pas la suite.

1. En utilisant `ping` suivi d'une adresse IP ou d'un nom de machine, pingez différentes machines et notez la connectivité. Un moyen simple de s'assurer qu'une machine fonctionne bien sur le réseau est de pinger l'hôte www.google.com ou son serveur DNS 8.8.8.8

La commande `netstat` est une commande importante qui vous permet de voir l'état des connexions actives sur votre machine, que ces connexions soient gérées par des socket réseau ou par des socket locales (dites UNIX). Générez un peu d'activité réseau (connexions web, ssh, etc.), puis testez les différentes commandes (aidez vous éventuellement du manuel) et notez à quoi correspondent ces quelques options :

```
$ netstat
$ netstat -n
$ netstat -a
$ netstat --tcp
$ netstat --inet --udp
$ netstat -r --inet -6
```

Comme vu en cours, toute application de type serveur utilise un port de communication et se met en attente d'une connexion entrante sur ce dernier. On souhaite savoir quels sont les couples (IP, port de communication) actuellement utilisés sur la machine. Pour cela répondez aux questions suivantes :

2. A quoi servent respectivement les options -a et -l de la commande `netstat` ?
3. En utilisant `netstat`, affichez la table des sockets en attente de connexions (état LISTENING) sans résolution des noms. Cette table n'est pas formatée comme suit selon les versions, mais doit présenter les mêmes éléments:

```
Current listen queue sizes (qlen/incqlen/maxqlen)
Listen         Local Address
0/0/5          *.88
0/0/1          *.4000
0/0/4          127.0.0.1.5037
0/0/5          *.2031
0/0/128        *.80
```

3. La politique de routage

La commande route permet de visualiser l'ensemble des politiques de routage de la machine sous forme d'une table de routage. Après avoir affiché la table de routage, répondez aux questions suivantes :

1. Quelle ligne de la table de routage correspond au routage du trafic entre les machines de la salle de TP dans laquelle vous vous trouvez?
2. A quoi sert une passerelle ? (anglais : *gateway*)
3. Quelle ligne de la table de routage va être considérée si l'on souhaite envoyer un message à l'adresse ip 80.80.80.80 ? Quel sera la prochaine machine à qui relayer le message, et par quelle interface devra-t'on lui envoyer le message ?
4. Quelle est la passerelle par défaut sur votre système?

4.Résolution des noms de domaine

Afin de faciliter l'utilisation du réseau, les machines peuvent être associées à un nom qui est généralement plus facile à retenir qu'une adresse IP. La résolution d'un nom est la conversion d'un nom sous forme d'adresse (ex: yahoo.fr) en une adresse IP (ex : 87.248.120.148). Cette résolution est opérée par un serveur distant, à qui l'on envoie une demande de résolution, et qui répond par l'adresse ip correspondante. Pour visualiser brièvement ces mécanismes, on utilisera la commande `nslookup`.

1. Exécutez la commande `nslookup` en lui passant comme paramètre un nom de machine (ex : www.yahoo.fr) et notez l'ensemble des éléments affichés.
2. Dans les résultats précédemment affichés, quel est l'adresse ip du serveur DNS ? Quelle est l'adresse IP de la machine www.yahoo.fr ?
3. Que contient le fichier `/etc/resolv.conf` ?
4. Notez qu'il est possible de se passer d'un serveur DNS si l'on indique au système d'exploitation la correspondance entre une adresse ip et un nom de domaine. Cette correspondance peut être écrite dans le fichier `/etc/hosts`.
5. En respectant le format présenté dans le fichier, ajoutez quelques entrées correspondant aux adresses IP des autres binômes, et pingez les à partir du nom que vous leur avez attribué.

III.Manipulations avancées

1.Etude d'une trame ethernet

La commande `ping` permet de «pinger» une machine, c'est à dire de lui demander si elle est active et reçoit bien les paquets qu'on lui envoie. Si l'hôte est actif, il répond en général en renvoyant le paquet envoyé. Le temps de transfert entre l'envoi du paquet et la réception du message est affiché à l'écran. Notons cependant qu'un hôte peut avoir désactivé la fonction de réponse, mais être quand même actif. D'apparence toute simple, la commande `ping` dispose d'une multitude d'options permettant de faire varier de nombreux paramètres.

1. Effectuez un `ping` sur les machines de la salle, puis sur l'adresse `yahoo.fr`. Notez le comportement de la commande et les temps de réponse associé. A quoi correspond le champ «`ttl`» ?
2. Lancer le programme `wireshark` avec les droits administrateur. Il s'agit d'un analyseur de trafic réseau (anglais : *network sniffer*) vous permettant de voir les différentes encapsulations opérées sur un message, chaque encapsulation étant associée à une couche du modèles TCP/IP.
   - Tentez quelques captures et manipulations pour découvrir ce logiciel;
   - En utilisant le tutoriel qui vous a été donné, appliquez un filtre ip, capturez le trafic, et dans une console pingez une machine de la salle. Notez l'ajout des nouveaux paquets dans l'interface de capture. Stoppez enfin la capture
3. En utilisant les paquets précédemment capturés, déterminez le protocole utilisé par l'envoi de paquet de types ping (et le numéro du type de paquet), la taille des en-tête pour chaque niveau d'encapsulation, dans quel champ se situe l'adresse ip du destinataire, et la valeur du ttl.
4. Recommencez l'opération de visualisation des paquets, mais cette fois en effectuant un ping sur l'hôte `google.fr` et en faisant varier le ttl. Que se passe-t'il lorsque le ttl est trop faible ? Quel est le type de message ? Regardez notamment attentivement l'adresse ip de la machine qui répond. Concluez sur le fonctionnement du ping et sur l'importance du ttl.
5. Pourriez-vous proposer une solution pour déterminer l'ensemble des adresses ip des routeurs qui se situent entre votre machine et un hôte dont l'adresse ip est donnée?
6. Sur un paquet de données HTTP, faites bouton droit «/ suivre le flux TCP pour reconstituer le paquet

2.La commande `traceroute`

Cette partie suppose que vous avez correctement répondu aux questions immédiatement précédentes. La commande `traceroute` effectue des ping successifs vers un hôte donné en incrémentant successivement le TTL.

1. Effectuez un ping vers l'hôte de votre choix (exemple : `bonifacio.fr`) et notez la liste des routeurs empruntés. Dans certaines situations, l'identité d'un routeur peut être masqué et représenté par trois étoiles plutôt que par son adresse IP. Proposez une explication à cela
2. effectuez un ping vers un hôte quelconque (par ex. yahoo.fr), et notez l'adresse IP du premier routeur emprunté. Cette adresse IP devrait elle normalement correspondre à l'adresse IP de la passerelle par défaut de votre table de routage ? Affichez votre table de routage et comparer les adresses IP. Ces adresses sont-elles identiques ? Quelle explication à cela?