Travaux Pratiques Réseau.

Informatique 2ème année: 2008/2009

—*Antoine Rollet* - `rollet@enseirb.fr` —

1 Quelques commandes

Voici quelques commandes qui vous seront utiles pour le TP :

1.1 Paquets

Vous êtes sur des distributions Debian qui repose sur une installation de logiciels se présentant sous la forme d'un paquet (en gros, une archive tgz améliorée).

Pour chercher un paquet à l'aide de mot clé la commande est :

```
>apt-cache search motcle
```

Pour obtenir la liste des paquets déjà installés :

```
>dpkg -l [pattern]
```

pattern peut être utilisé pour filtrer la liste.

Pour obtenir la description d'un paquet :

```
>apt-cache show nompaquet
```

Enfin, pour installer un paquet :

```
>apt-get install nompaquet
```

1.2 Interfaces

La manipulation des interfaces réseaux se fait à l'aide de la commande `ifconfig`. Pour obtenir les informations sur l'ensemble des interfaces disponibles sur le système :

```
>ifconfig -a
```

Sans l'option `-a`, la commande n'affichera que les interfaces actuellement active.

On active/désactive une interface à l'aide des commandes :

```
>ifup iname
>ifconfig iname up
>ifdown iname
>ifconfig iname down
```

Voici une commande typique pour configurer une interface :

```
>ifconfig eth0 192.168.10.5 netmask 255.255.252.0 broadcast 192.168.13.255
```

Remarque :

1. Si on ne spécifie par l'adresse de diffusion, la commande le calcule toute seule en fonction de l'adresse ip et du masque.
2. Si le masque n'est pas spécifié, celui-ci est calculé en fonction de la classe de l'adresse.
3. Une entrée correspondante au réseau associé à l'interface est automatiquement ajoutée dans la table de routage.

Pour connaître l'état des interfaces (au niveau physique) des outils sont disponibles :

```
>mii-tool
>mii-diag
>ethtool
```

Toutes ces commandes ne sont pas nécessairement installées par défaut.

1.3 Table de routage

Pour manipuler la table de routage on utilise la commande `route`.

Voici quelques exemples de commandes valides :

```
>route -n
>route add default gw 193.140.10.1
>route add -host 192.168.10.2 dev eth2
>route add -host 192.168.10.3 gw 192.168.10.1
>route add -net 128.0.0.0 netmask 128.0.0.0 gw 192.168.10.1
>route del -host 192.168.10.2 dev eth2
```

Une autre commande très utile est la commande `ip`. Celle-ci permet de faire des manipulations au niveau de la couche ip. Voici quelques exemples de commandes en rapport avec la table de routage, se référer à la page de manuel pour plus d'informations :

```
>ip route flush all
>ip route list
>ip route get 192.168.10.1
>ip route get 209.85.135.104
```

Enfin, la commande `netstat` permet elle aussi d'obtenir des informations sur le réseau :

```
>netstat -rnv
```

2 Le TP

2.1 Prise en main

Le TP se fait par groupe de 4 personnes, chaque groupe a à sa charge la configuration de 2 machines côte à côte. Les groupes sont numérotés comme ci-dessous :

1	5
2	6
3	7
4	8

Dans la suite on désignera par **passerelle d'un groupe** la machine côté couloir, et **machine cliente** la machine côté mur. Enfin la **passerelle principale** est la machine à l'entrée de la salle.

Initialement, toutes les machines sont connectées à la passerelle principale à travers un switch.

Tout au long du TD, le tableau servira à représenter l'état de la configuration de la salle. Doivent apparaître notamment : les interfaces, les 2 derniers octets des adresses physiques, les tables de routage, les propriétés des réseaux.

Pour chaque machine, donner : (commande à utiliser : `ifconfig, route, arp`).

- l'interface par laquelle elle est connectée au réseau local.
- Pour cette interface donner :
  - l'adresse physique
  - l'adresse ip
  - l'adresse réseau
  - le masque réseau
  - l'adresse de diffusion
- l'adresse ip de la passerelle principale
- l'adresse physique de la passerelle principale

Mettre à jour le tableau.

2.2 Configuration

Débrancher la machine cliente du réseau local de la salle.

En utilisant les câbles à côté des machines, relier la machine cliente à sa passerelle. Il est possible de les relier soit directement, soit à l'aide d'un HUB. Ici prendre un hub.

À l'aide de `mii-tool` vérifier quelles sont les interfaces connectées sur la machine cliente ainsi que sur la passerelle.

On rappelle que dans la classe C, les adresse 192.168.x.y sont réservées pour un usage privé.

Pour chaque groupe i (i allant de 1 à 8), configurer le réseau local entre le client et la passerelle de groupe en utilisant l'adresse de réseau $192.168.16 * (i-1).0$. Vous donnerez l'adresse la plus basse à la passerelle et l'adresse la plus haute au client.

Mettre à jour le tableau, puis modifier la configuration des machines.

Vérifier que le client et sa passerelle communiquent bien à l'aide de la commande `ping`. Essayer de communiquer avec la passerelle principale depuis la passerelle de groupe et depuis le client.

Pour autoriser les paquets entrant sur une interface réseau à transiter sur une autre interface réseau, il faut activer l'IP forwarding (fonction de passerelle).

Linux propose un répertoire appelé "système de fichiers virtuels" et qui contient des fichiers virtuels, il s'agit du répertoire "/proc". La plupart des fichiers ont une longueur de zéro et ne nous intéressent pas. Par contre les répertoires "/proc/filesystems" et "/proc/sys/" contiennent des informations de configuration système. Ainsi, on trouve dans "/proc/sys/net/ipv4" des fichiers permettant de configurer la pile TCP/IP. Pour activer l'ip forwarding, il suffit que le fichier "ip_forward" contienne la valeur "1", et pour désactiver il suffit de mettre un zéro.

Vérifiez si l'IP forwarding est activé sur la passerelle. Sinon activez-le.

Re-vérifier la communication entre le client et la passerelle principale (`ping`). On pourra lancer le programme `wireshark` sur la passerelle de groupe afin de voir passer les données. Indiquer le cheminement des données à travers le réseau. Quel est le problème ?

Si vous aviez la main sur la passerelle principale, quelle serait une solution possible (`route`) ?

Mettez en place une solution afin que chaque groupe i puisse communiquer avec le groupe $i+4$. Vérifier alors que le client du groupe i peut bien communiquer avec le client du groupe $i+4$.

Afin d'optimiser les tables de routage, nous allons couper la salle en deux : les groupes 1 à 4 et les groupes 5 à 8. Pour le groupe i, la passerelle du groupe $i+4$ doit servir de passerelle pour tous les réseaux de 5 à 8.

Réciproquement la passerelle du groupe i doit permettre au groupe $i+4$ d'atteindre les groupes 1 à 4.

Mettre à jour le tableau. Effectuer la modification et tester les communications (à la fin tous les clients doivent pouvoir communiquer entre eux).

2.3 Configuration Automatique

La configuration réseau effectuée au paragraphe précédent n'est pas permanente. Elle est réinitialisée à chaque redémarrage du service réseau. Il faut modifier un fichier de configuration système qui est lu et interprété lors de l'exécution des scripts de démarrage.

Sur chaque machine, éditez le fichier `/etc/network/interfaces` et ajoutez-y les lignes :

```
auto ethi
iface ethi inet static
address address
netmask netmask
network network
broadcast broadcast
gateway gateway
```

Vous pourrez vous référer à la page de manuel pour plus de détails (`man 5 interfaces`). Tester votre configuration en redémarrant le service `/etc/init.d/networking restart`.

Si on redémarre la machine, vous verrez que la configuration des interfaces est bien maintenue, par contre la table de routage a été perdue. Pour conserver celle-ci vous avez deux solutions :

– Ajouter les commandes `route` dans la section `ethi` en la préfixant de `up` :

```
iface eth2 inet static
    address 172.23.100.23
    up route add -net 192.168.16.0 gw 172.23.100.24
```

– Ajouter un script dans le répertoire `/etc/network/if-up.d`. Cette solution étant plus complexe, nous ne l'utiliserons pas.

Enfin, l'ip forwarding n'est pas non plus maintenue. Vous avez deux solutions, ajouter une ligne `up echo 1 > /proc/sys/net/ipv4/ip_forward` dans le fichier `interfaces` ou bien ajouter la ligne

```
net.ipv4.ip_forward=1
```

dans le fichier `/etc/sysctl.conf`.

2.4 Wireshark

Pour finir, nous allons aborder quelques aspects de sécurité.

Installer un serveur FTP sur la passerelle. Pour cela, on pourra utiliser la commande :

```
>apt-get install proftpd
```

Éditer le fichier `/etc/proftpd/proftpd.conf` afin d'activer le service et d'ajouter un utilisateur.

Nous allons maintenant voir comment une machine hostile peut intercepter des informations sensibles. Nous allons simuler un hôte qui "sniffe" le réseau...

Sur le client brancher l'interface encore non utilisée (eth0 ou eth1) sur le hub. L'activer. Lancer à l'aide de Wireshark (ou tcpdump) une capture des trames sur cette interface. Pour cela, lancer la commande `wireshark`. Puis dans le menu, cliquer sur `capture` puis `start`. Cette partie du client sera appelée "espion".

Toujours sur le client (mais pas l'espion...), essayer de se connecter au serveur ftp (login + mot de passe). Sur l'espion, essayez d'identifier le login et le mot de passe.

Proposez des solutions pour résoudre cette faiblesse de sécurité (les essayer si possible).

2.5 DHCP

On va maintenant changer la configuration des postes clients en leur attribuant une adresse IP (et autres informations réseaux) dynamiquement par DHCP, au lieu de statiquement comme réalisé au-dessus.

Le protocole DHCP est un protocole dans lequel une machine demande ses paramètres ip en faisant un broadcast. Il se base sur UDP. Si un serveur est disponible sur le réseau du client, il peut lui répondre et lui fournir sa configuration réseau.

2.5.1 Coté serveur

Installez le paquet `dhcp3-server` sur la passerelle.

Par défaut le serveur DHCP est configuré sur eth0. Pour modifier ultérieurement cette interface, il est possible de faire `dpkg-reconfigure dhcp3-server` ou de modifier le fichier `/etc/default/dhcp3-server`.

Le fichier de configuration du serveur dhcp est `/etc/dhcp3/dhcpd.conf`. Faites en une copie de sauvegarde et changez les valeurs qu'il faut.

Donnez les valeurs que vous avez configurées.

Ne pas oublier de redémarrer le démon pour prendre en compte les modifications :

```
/etc/init.d/dhcp3-server restart
```

S'il y a une erreur, regardez dans le fichier `/var/log/messages`.

Pour avoir des adresses IP fixes avec le serveur DHCP en fonction des adresses MAC, il faut renseigner le fichier `/etc/dhcp3/dhcpd.conf` avec les éléments suivants :

```
host INFO-TG {
 hardware ethernet @MAC;
 fixed-address @IP;
}
```

2.5.2 Coté client

Enlevez la configuration réseau statique du client. Pour configurer un poste client sous Linux, il faut modifier le fichier :

/etc/network/interfaces

Ce fichier doit contenir :

```
auto lo ethi
iface lo inet loopback
iface ethi inet dhcp
```

(Noter le `dhcp` à la place du `static`).

Il ne faut pas oublier de redémarrer le démon après modification :

```
/etc/init.d/networking restart
```

2.5.3 Fichier dhcp

Sur le client et le serveur, regarder le contenu du répertoire `/var/lib/dhcp3/`. Inspecter les différents fichiers.