TP Réseau : Interface IP

Les TP d'acquisition des fondamentaux visent à construire un socle de connaissances de base, à appréhender des concepts, des notions et des modèles qui sont fondamentaux. Ce sont des étapes indispensables pour aborder d'autres apprentissages. Les TP sont conduits de manière fortement guidée pour vous placer le plus souvent dans une situation de découverte et d'apprentissage.

Objectifs

Les objectifs de ce TP sont de découvrir la communication réseau IP :
- prendre en main le fonctionnement de netkit
- observer la communication entre deux machines dans un même réseau local
- configurer les paramètres IP d'une machine sous Linux
- étudier le fonctionnement des protocoles de la couche réseau (IP, ICMP, ARP)
- utiliser les commandes de configuration IP et de test
- se sensibiliser aux risques et à la sécurité du réseau

TP Réseau : Interface IP

Travail préparatoire

Installation du TP

Le TP1 est disponible dans l'archive `/home/user/sujets-tp/tp1.tgz` :

```
host> tar zxvf sujets-tp/tp1.tgz
```

Le prompt `host>` indiquera que la commande doit être tapée dans le terminal de votre machine réelle (par opposition aux terminaux ouverts par les machines virtuelles). Par exemple, votre terminal distant `ssh`. Le prompt `name:~#` représentera le terminal de la machine virtuelle `name`.

Démarrage des machines virtuelles

Démarrer le premier tp en lançant la commande `lstart` (`-s` pour le mode séquentiel) dans le répertoire du *lab* (ici `tp1`) :

```
host> cd /home/user/tp1
host> lstart -s
```

Remarque : il est conseillé de lire la FAQ Netkit fournie.

La maquette

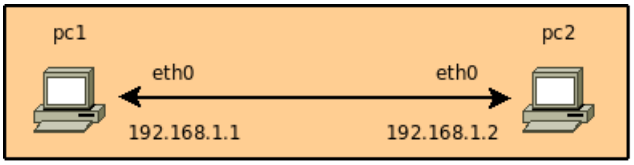
Dans ce TP, on dispose de deux machines (`pc1` et `pc2`) reliées entre elles :

```
pc1[0]="A"
pc2[0]="A"
```

Le fichier lab.conf

Le numéro précise l'interface utilisé : ici 0 → `eth0`. La lettre identifie le domaine de collision (virtuel) sur lequel les machines `pc1` et `pc2` échangeront des trames : ici le domaine de collision est nommé `A`.

Ce qui donne le schéma suivant pour le réseau **192.168.1.0/24** :



Dans Netkit, le concentrateur (*hub*) est transparent. Il suffit de relier des machines sur un même domaine de collision (virtuel) pour qu'elle puisse échanger des trames. Il sera possible par la suite de capturer (*sniffer*) les trames échangées sur un domaine de collision en précisant son nom.

```
host> vdump A | wireshark -i - -k &
```

Configuration

Sous GNU/Linux, la commande `ifconfig` permet la configuration des interfaces réseaux.

```
pc1:~# ifconfig eth0 up
pc1:~# ifconfig eth0
```

Activer et visualiser les paramètres de `eth0`

Pour configurer l'interface `eth0` de chaque machine, on utilisera donc la commande `ifconfig` en précisant l'adresse de diffusion générale (*broadcast*) et le masque réseau (*netmask*) :

```
pc1:~# ifconfig eth0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255

// Ou :

pc1:~# ifconfig eth0 192.168.1.1/24
```

Sur les distributions Debian/Ubuntu, le fichier `/etc/network/interfaces` gère la configuration des interfaces au démarrage du service réseau, par exemple pour l'interface `eth0` :

```
auto eth0
iface eth0 inet dhcp
```

Adressage dynamique par DHCP

Ou :

```
auto eth0
iface eth0 inet static
address 192.168.3.1
netmask 255.255.255.0
broadcast 192.168.3.255 # optionnel
gateway 192.168.3.254 # optionnel
```

Adressage statique

Si le fichier est modifié, il faudra relancer le service réseau :

```
pc1:~# service networking restart

// ou :

pc1:~# /etc/init.d/networking restart
```

Test de communication

Pour réaliser un test de base d'une liaison réseau, on utilise souvent la commande `ping` qui permettra, en cas de succès, de valider la pile de protocoles jusqu'au niveau IP.

```
pc1:~# ping 192.168.1.2 -c 1
```

pc1 envoie un message ICMP de type *echo request* auquel la machine **pc2** va répondre par un message ICMP *echo reply*. Pour connaître les options de la commande `ping`, consulter les pages `man`.

ICMP est un protocole de couche Réseau, qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoi de messages d'erreur, c'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau (par exemple lorsqu'un service ou un hôte est inaccessible). Il est détaillé dans la **RFC 792**.

Travail demandé

L'interface réseau

Question 1. Configurer les paramètres IP des interfaces de `pc1` et `pc2`.

Question 2. Relever l'adresse MAC de vos deux cartes réseau.

Question 3. Donner la commande `ping` pour tester une communication depuis **pc2** vers **pc1**.

Question 4. Éditer le fichier de configuration du poste **pc2** et ajouter la configuration **192.168.1.3** pour `eth0`. Donner la syntaxe exacte des lignes que vous avez ajoutées.

> Vous pouvez utiliser l'éditeur de texte `vim`. Pour insérer du texte, il faut taper **i**. Pour sortir du mode édition, appuyez sur **Echap** puis taper `:wq` pour enregistrer et sortir de l'éditeur.

Question 5. Relancer le service réseau en donnant la commande que vous avez utilisé. Vérifier que la nouvelle adresse a bien été prise en compte.

Question 6. Observer les valeurs des registres **TX/RX** avec la commande `ifconfig`, avant et après avoir exécuté la commande `ping localhost`. Par quelle interface passent les paquets émis par la commande `ping localhost` ? Quel est son nom ?

Question 7. Tester l'état de connexion vers une adresse IP inexistante de votre réseau. Puis, vers une adresse IP inexistante d'un autre réseau. Donner les commandes et commenter les réponses obtenues.

Le protocole ICMP

Activer une capture `wireshark` lors d'un `ping`.

Question 8. Quelle est la valeur du champ *Protocol* de l'en-tête du paquet IP ? Quel est le protocole de plus haut niveau utilisé par la commande ?

Question 9. Donner alors la pile de protocoles mise en oeuvre par cette commande.

Question 10. Quels sont le **type** et le **code** des requêtes et réponses échangées par le protocole de plus haut niveau ?

Question 11. Que signifie `rtt` dans l'affichage des statistiques de la commande `ping` ?

Les options concernant le réseau et donc le protocole ICMP sont accessibles depuis le répertoire `/proc/sys/net/` :

```
pc1:~# find /proc/sys -name *icmp* | grep ipv4
/proc/sys/net/ipv4/icmp_echo_ignore_all
/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
/proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
/proc/sys/net/ipv4/icmp_errors_use_inbound_ifaddr
/proc/sys/net/ipv4/icmp_ratelimit
/proc/sys/net/ipv4/icmp_ratemask

// Pour visualiser la valeur d'une option, on réalise l'opération suivante :
pc1:~# cat /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
1
```

```
// Pour modifier la valeur d'une option booléenne, on fera (0=inactif et 1=actif) :
pc1:~# echo "0" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
pc1:~# cat /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
0
```

Question 12. Modifier l'option qui permettra d'interdire toute réponse ICMP de type `echo reply` pour le poste **pc2**. Donner la commande et vérifier son efficacité.

Question 13. Donner la syntaxe de la commande `ping` qui permet d'envoyer à tous les postes de votre réseau depuis **pc1**. Comment se nomme cette technique ? Fonctionne-t-elle ?

Le protocole ARP

Question 14. Vider le cache `arp` de votre machine par une commande `arp -d`. Puis exécuter une commande `ping` depuis **pc1** vers **pc2**.

Question 15. Pourquoi visualisez-vous des trames ARP sur votre capture ?

Question 16. Observer l'adresse MAC de destination d'une requête ARP. Expliquez sa valeur. Quels sont les deux types de paquet ARP ?

Question 17. Quel est maintenant le contenu du cache ARP des postes **pc1** et **pc2** ?

Question 18. Sur **pc2**, utiliser la commande `arp -s` pour modifier l'adresse matérielle associée à **pc1**. Donner une fausse adresse, par exemple 08:00:02:22:22:20.

Question 19. Faire un `ping` de **pc2** vers **pc1**. Noter et expliquer le résultat obtenu.

Question 20. Sachant que des générateurs de paquets ARP (comme `arpspoof`, `nemesis`, `Scapy`, ...) existent, quels sont alors les risques liés au protocole ARP ? Quel est le nom donné à la technique utilisée ici ?