TP Réseaux avec Marionnet : Routage statique et Adressage, Initiation pare-feu

Franck Butelle
Université Paris 13

2011

Ce TP utilise le logiciel **marionnet** développé à Paris 13, voir www.marionnet.org.
Vous utiliserez la commande man pour chercher les options des commandes qui vous seront nécessaires.

1 Créez un nouveau projet

Dans ce projet ajoutez deux machines virtuelles (m1 et m2 avec les valeurs par défaut) non reliées et lancez-les par exemple par le bouton "tout démarrer". Configurez les adresses IP de ces deux machines par la commande :

`ifconfig <interface> <adresseIP>` `[netmask <masque réseau>]`

L'interface est `eth0` ou `eth1` etc. Les paramètres entre crochets (et en surligné gris) sont optionnels. Si le netmask n'est pas fourni, le système le calcul automatiquement.
Les machines doivent avoir le même numéro de réseau de classe A.

2 Reliez ces machines

- Essayez un câble droit et un câble croisé, comment vérifier que la liaison fonctionne ?
- Consultez le cache ARP avec la commande `arp -a`. Que contient-il ?

Reliez maintenant ces machines par un HUB (concentrateur), pensez à démarrer ce HUB !

3 Comparaison HUB et Switch, étude de ARP

Ajoutez une 3e machine que vous appellerez `Espion`. Démarrez-la et lancer dessus l'analyseur de trames `wireshark` (ou **ethereal**), patientez son lancement peut être lent !. Une fois wireshark lancé, faites un ping entre m1 et m2.

- Que constatez-vous ? Regardez en particulier les diodes du HUB.
- Pourquoi voit-on des paquets ARP avant les paquets ICMP ?

Supprimez les entrées dans les caches ARP de m2 par `arp -d`.
Changez l'entrée dynamique du cache ARP de m1 par une entrée statique équivalente (voir `arp -s`).
Testez à nouveau ping en lançant l'analyseur au préalable.

- Que constatez-vous ?

Supprimez les entrées du cache ARP et relancer le `ping` puis regardez à nouveau le cache ARP...

- Qu'y a-t-il dans la partie donnée des paquets ICMP ?

Arrêtez le ping, relancez-le avec une option qui permette de changer le contenu des paquets ICMP par le motif (pattern) 0xBA répété (utile pour détecter des erreurs de transmissions dépendantes des données).

- Voyez-vous ces paquets dans l'analyseur ? Pourquoi ?
- Consultez le cache ARP de chaque machine. Quelle est l'adresse MAC de Espion ?
- Changez maintenant le HUB par un *Switch* (Commutateur niveau 2), que constatez-vous du côté des diodes ? Pourquoi ? Et au niveau de l'analyseur ?

Si vous n'avez pu voir le phénomène, il faut essayer de donner à Espion une adresse IP dans le même réseau et tester un ping à partir de lui...

4 Broadcast

Pour toute la suite il faut remplacer le Switch par un HUB.

Donnez à Espion une adresse IP sur le même réseau que M1 et M2. Sur M2 et Espion les broadcast sont refusés par défaut pour des raisons de sécurité. Il faut changer cela par :

```
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts = 0
```

(`sysctl` est utilisé pour modifier les paramètres du noyau en cours d'exécution). Depuis M1, lancer un ping en broadcast sur le réseau.

- Quelle est la commande à taper ?

5 Fragmentation

Les cartes réseaux Ethernet sont réglées par défaut pour respecter Ethernet, c'est à dire une MTU de 1500 octets.

- Que veux dire MTU ? Vérifiez sa valeur actuelle sur M1 et M2.

Avec une option spéciale de ping on peut faire des paquets presque aussi gros que l'on veut.

- Quelle est cette option ?

Utilisez-la pour faire un ping de 1500 octets entre M1 et M2.

- Pourquoi il y a-t-il alors de la fragmentation ?

Avec l'analyseur consultez la taille des fragments en regardant la valeur offset (l'analyseur l'affiche en octets et non en nombre de mots de 8 octets).

- Est-ce correct par rapport à ce que l'on a vu en TD ?

On peut aussi changer le MTU de M1 et M2 par `ifconfig`.

- Si les paquets ICMP sont de 500 octets, quel est le MTU minimum pour qu'il n'y ait pas de fragmentation ? Vérifiez !

6 Routage statique

Nous allons ici utiliser un PC avec 2 cartes réseaux comme routeur.

Arrêtez la machine espion et supprimez là. Créez une nouvelle que vous appellerez « routeur », avec **2 cartes réseaux**. Démarrez cette machine et vérifiez que vous avec 2 cartes avec ifconfig :

- Quelles sont les adresses MAC des cartes réseaux de la machine « routeur » ?

Reliez M1 à `eth0` de routeur et M2 à `eth1` de routeur.

Testez par ping les liens M1→ Routeur et M2→Routeur. Le routage n'est pas activé par défaut sur une machine normale (sur les vrais routeurs c'est différent). Nous allons l'activer par :

```
sysctl -w net.ipv4.ip_forward = 1
```

(Pour désactiver le routage, mettre 0 à la place de 1 !)

- Maintenant tester le ping de M1 à M2, que manque t-il encore ?

Vous pouvez consultez les tables de routage par la commande `route`. Pour ajouter une entrée dans la table de routage :

`route add -net <destination> [netmask <masque réseau>] [gw <adresseIP>] <interface>`

Pour ajouter une route par défaut, la syntaxe est simplifiée :

`route add default gw <adresseIP>`

Pour supprimer une route :

`route del ...`

Ajoutez ce qu'il faut jusqu'à ce que le ping marche dans les deux sens. Note : il n'est pas nécessaire d'avoir une route par défaut sur le routeur...

Lancez `wireshark` sur le routeur, vous devriez pouvoir voir passer les trames...

7 Tracer la route

Depuis M1 faites `traceroute` (ou `tracepath`) <adresseIP> où *adresseIP* est l'adresse de M2.

- Donnez la route suivie par le paquet.

Sur le routeur ajoutez une route par défaut via l'interface eth0 avec l'adresse de M1 en guise de passerelle ! Testez par `traceroute adresseIPbidon` à partir de M2 avec wireshark lancé sur le routeur.

- Notez sur votre compte-rendu la commande que vous avez tapé et le résultat, essayer d'expliquer ce comportement. Donnez la route suivie par le paquet.

Supprimez la route par défaut que vous avez ajouté sur le routeur et désactiver le routage sur M1.

8 Initiation aux règles de paramétrage d'un Pare-Feu ("Firewall")

A partir de M2 lancez `lynx` (un navigateur en mode texte !) avec comme paramètre l'adresse IP de M1. Normalement la connexion s'établit (sinon essayez de relancer le service sur M1 avec `/etc/init.d/apache2 restart`).

Sur le routeur tapez les commandes suivantes :

```
iptables -A FORWARD -s adresseIPdeM1 -j LOG
iptables -A FORWARD -s adresseIPdeM1 -j REJECT
```

(`-A` signifie Append, `-s` : sourceAddress ; `-j LOG` : garde trace les paquets correspondant à cette règle ; `-j REJECT` rejet de tout paquet IP correspondant à cette règle).

Afficher la liste des règles sur les paquets entrants : `iptables -L INPUT`

Supprimer toutes les règles : `iptables -F`

Essayez de nouveau de lancer un `ping` vers l'adresse IP du routeur. De même avec un telnet.

- Tapez `tail /var/log/messages` sur le routeur. Que constatez-vous ?
- Ajoutez une règle pour ne filtrer que les messages TCP :

`iptables -A FORWARD -s adresseIPdeM1 -p tcp -j REJECT`

Testez à nouveau avec votre navigateur et `ping`... puis supprimez la règle que vous avez ajouté par la commande précédente.

Question : Quelle serait la règle pour rejeter tout paquet ICMP, quelque soit l'adresse source ?