M2102-- TP1

Configurer les interfaces réseaux -- la commande ifconfig

Nous allons travailler sur Linux. Dans cet environnement la configuration des interfaces réseaux se fait en utilisant la commande ifconfig. Cette commande ne s'utilise qu'en tant que root. Parmi les options qu'on peut choisir pour cette commande nous avons :

- `ifconfig` : sans option, cette commande nous rend les interfaces actives avec leurs configurations
- `ifconfig -a` : avec cette option, nous allons voir toutes les interfaces disponibles, qu'elles soient actives ou non, configurées ou non.
- `Ifconfig <nom d'interface>` : affiche la configuration actuelle de l'interface nommée
  Exemple : `ifconfig eth0`
- `Ifconfig <nom d'interface> <up ou down>` : active ou désactive l'interface nommée
  Exemple : `ifconfig eth0 up`
- `Ifconfig<nom d'interface> <adresse IP /CIDR réseau>` : configure l'interface nommée à l'adresse IP et réseau mentionnés
  Exemple : `ifconfig eth0 192.168.57.2/24`
- `Ifconfig <nom d'interface> <adresse IP> netmask <masque>` : même que ci-dessus
  Exemple : `ifconfig eth0 192.168.57.2 netmask 255.255.255.0`

La configuration d'une adresse IP avec cette commande indique implicitement le réseau dans lequel la machine peut communiquer directement. Notamment si on configure l'interface `eth0` à `192.168.26.3/24`, cette machine pourra communiquer directement par cette interface à toute machine dans le réseau `192.168.26.0/24`, tandis que si on la configure à `192.168.26.3/25` elle ne pourra communiquer directement qu'aux machines dans le réseau `192.168.26.3/25`.

Vous pouvez trouver plus d'informations sur la commande `ifconfig` en utilisant la commande `man ifconfig`

Vérifier la connectivité -- la commande ping

La commande ping nous permet de vérifier la connectivité entre deux machines. Le protocole de ping consiste en deux types de messages : un message de type ping request, qui part d'une machine et essaie de joindre une deuxième machine, et un message de type ping response, qui fait le chemin inverse.

Pour faire un ping d'une machine A à une machine B, dont on connaît l'adresse IP, il faut utiliser la commande ping avec l'une des options suivantes :

- ping <adresse IP de la machine B> : fait des pings vers la machine ciblée jusqu'à une intervention, comme par exemple CTRL + C
- ping -c <nombre de pings> <adresse IP de B> : fait un nombre spécifique de pings vers la machine ciblée.

La capture des messages réseau -- le logiciel Wireshark

Dans le cadre de ce module nous allons également apprendre comment examiner les messages échangés par plusieurs machines en utilisant l'outil Wireshark. Cet outil nous permet de faire une capture sur les messages reçus ou envoyés par une machine qui fonctionne en réseau. Les captures ne peuvent être faites que lorsque la machine est en-ligne, mais une capture peut également être analysée hors-ligne.

Nous allons utiliser ce protocole pour :

- Examiner des éléments de l'encapsulation des messages
- Comprendre la structure d'un paquet (qui transmit à qui et comment)
- Analyser le déroulement de divers protocoles
- Comprendre la source des erreurs en réseau

Pour utiliser ce logiciel nous allons devoir démarrer une capture sur le réseau. Pour ce faire il faut choisir les interfaces sur lesquelles nous voulons faire une capture, puis faire un click sur Start. Nous pouvons arrêter la capture à chaque instant, en utilisant le bouton dédié sur la barre de menu.

Au-delà de juste intercepter/capturer les messages envoyés et reçus par une machine, Wireshark a la capacité de les analyser, en extrayant les informations utiles à chaque couche et en les affichant sur son interface graphique.

Démarrer le TP

Vous allez démarrer le TP en utilisant les instructions données dans le préambule : vous allez premièrement importer la machine virtuelle en vérifiant que vous avez bien coché la caisse qui assure la réinitialisation des adresses MAC. Ouvrez un terminal.

Exercice 1

Vous allez commencer le travail par rangée, avec 4 machines et 3 ou 4 étudiants par rangée. Si vous êtes à moins de 4 personnes, vous allez pourtant devoir faire le travail sur toutes les machines sur votre rangée.

Chaque rangée commence ce TP en choisissant son propre réseau privé de classe C, qui devra être différent de celui des autres rangées.

1. Dès que vous avez choisi le numéro de votre réseau, écrivez-le sur le tableau en notation CIDR et avec un masque de réseau. Premier arrivé premier servi.
   Ecrivez le numéro de réseau ci-dessous également :

   - Notation CIDR :
   - Masque de réseau :

2. Listez toutes les interfaces disponibles de votre machine.

   Commande utilisée :

   Résultat :

3. Quel résultat obtenez-vous si vous utilisez la même commande que tout-à-l 'heure, toutefois sans y ajouter aucune option ?

   Commande utilisée :

   Résultat :

   Justification du résultat :

4. Pour chaque machine dans votre rangée, **configurez l'interface eth1** pour qu'elle ait une des numéros de machine suivants (chaque adresse doit apparaître une fois et une fois seulement sur votre rangée). Ecrivez à côté de chaque numéro de machine le numéro sur le boîtier de chaque machine, ainsi que la commande que vous allez taper là-dessus.

   44

   135

195

234

5. Utilisez la commande ping pour vérifier la connectivité entre vos quatre machines. Indiquez dans le tableau ci-dessous leur connectivité.

Connectivité	44	135	195	234
44				
135				
195				
234				

6. Maintenant vous allez partager votre réseau dans deux sous-réseaux de taille égale. Chaque machine aura encore le même numéro de machine, mais cette fois-ci dans un de ces deux sous-réseaux.

   Les adresses de ces deux sous-réseaux sont :
   - Premier sous-réseau
   - Deuxième sous-réseau

   Commande à taper sur votre machine pour la configurer :

7. Utilisez la commande ping pour revérifier la connectivité dans votre nouveau réseau.

Connectivité	44	135	195	234
44				
135				
195				
234				

8. Comment pouvez-vous justifier ces résultats ?

9. Remodifiez le réseau pour diviser chacun de vos sous-réseaux actuels en deux parties égales. Ceci devrait vous donner un total de quatre sous-réseaux sur chaque rangée.

   Donnez les adresses des quatre sous-réseaux que vous avez obtenus :
   - Premier sous-réseau :
   - Deuxième sous-réseau :
   - Troisième sous-réseau :
   - Quatrième sous-réseau :

   Votre machine devrait être configurée avec le même numéro de machine que dans les exercices précédents, mais dans le réseau plus petit. Quelle est la commande que vous allez taper ?

10. Est-ce que les quatre machines (44, 135, 195, 234) se trouvent chacune dans son propre sous-réseau ? Sinon, quel(s) réseau(x) contient (contiennent) plus qu'une seule machine ?

11. Comment pourrait-on s'assurer qu'on a une seule machine per sous-réseau ?

Exercice 2

1. Nous allons ensuite changer l'adresse de la machine 44 du sous-réseau considéré pour la question 9 au réseau de classe C considéré dans la question 1.

   Quel est le réseau de la machine 195 (quelles machines inclut-il ?)

   Quel est le réseau de la machine 44 ?

   Disons qu'on voulait faire un ping de la machine 44 vers la machine 195. Quel serait le fonctionnement du protocole et le résultat attendu ? Justifiez votre réponse.

2. Nous allons essayer de vérifier la connectivité entre les machines 44 et 195.

   Faites premièrement un ping de la machine 44 vers la machine 195. Quel est le résultat ?

   Ensuite faites un ping de la machine 195 vers la machine 44. Quel est le résultat ?

   Pouvez-vous justifier les deux comportements observés ?

3. Nous allons vérifier nos hypothèses (pour les questions précédentes) en utilisant le logiciel Wireshark. Trouvez ce logiciel sur votre machine et faites démarrer une capture Wireshark sur les machines 44 et 195. Utilisez la même commande ping que vous avez utilisé dans la première question.

   Trouvez sur la capture Wireshark une trame qui correspond au protocole ping utilisé.

4. Faites maintenant un ping inverse, de la machine 195 vers la machine 44.

   Pouvez vous trouver une trame correspondante à cette commande sur la machine 44 ?

   Et sur la machine 195 ?

5. Expliquez le comportement que vous avez observé.

Exercice 3

A partir de maintenant vous allez travailler chacun sur sa propre machine. Modifiez la configuration IP de votre réseau pour utiliser l'adresse IP sur le boîtier + 20 (voire le Préambule).

1. Quelle commande avez-vous utilisé ?

2. Consultez la cache ARP actuelle de votre machine en utilisant la commande :

   arp -a

   Si la table n'est pas vide, utilisez la commande suivante pour chacune des lignes présentes dans votre tableau :

   arp -d <adresse IP dans le tableau>

3. Si vous vouliez faire un ping et un seul vers la machine de l'enseignant dans votre salle, quelle serait la commande utilisée ?

4. Lancez Wireshark. Lancez une nouvelle capture en choisissant l'interface utile. Tapez la commande indiquée à l'exercice précédente. Arrêtez la capture.
   Analysez les trames ARP échangées et relevez les détails suivants :

   - L'adresse IP de votre machine
   - L'adresse IP de la machine de l'enseignant
   - L'adresse MAC de votre machine
   - L'adresse MAC de la machine de l'enseignant

5. Vérifiez que cet échange a ajouté l'adresse MAC de la machine de l'enseignant sur votre machine. Quelle commande faut-il taper pour cela ?

6. Trouvez dans la capture les commandes ping.
   - Quel est le protocole utilisé par la commande ping ?
   - Quelle est l'encapsulation (pile de protocoles) utilisés par ce protocole ?

Exercice 4

Finalement nous allons essayer de connecter la machine vers l'Internet. Pour ce faire, notre machine aura besoin de connaître la passerelle à utiliser pour sortir du réseau. Utilisez la commande suivante :

route add default gw <adresse de la passerelle dans votre salle, voir préambule>

Videz la cache ARP de votre machine si elle n'est pas encore vide. Relancez une capture Wireshark. Faites un ping et un seul vers l'adresse IP 8.8.8.8, puis arrêtez la capture.

1. Analysez les trames ARP échangées et trouver :

   - L'adresse IP de la machine ciblée
   - L'adresse MAC de la machine ciblée :

   Pouvez-vous deviner qui est cette machine ?

2. Etudiez les trames de ping. Relevez les informations suivantes concernant la machine de destination :

   - L'adresse IP de la machine
   - Quelle est la machine dont on indique l'adresse IP ?

   - L'adresse MAC de la machine
   - Quelle est la machine dont on indique l'adresse MAC ?

3. Et l'adresse MAC de la destination, c'est-à-dire la machine dont l'adresse IP est 8.8.8.8 ?