R2.04-- TP1

Conseils sanitaires covid19 (lisez tout ça !)

Ce TP demande de la collaboration entre vous (équipes de 3-4 étudiants).

Il est strictement interdit de :

- travailler sur une même machine qu'un autre étudiant (partage de clavier, souris, toucher l'écran)
- toucher à plusieurs un même périphérique de réseau (câbles, switches, etc.)
- ne pas porter votre masque tout le temps et correctement

Par contre, ce qui est permis (même encouragé) :

- la communication entre vous (en gardant bien sûr la distance de sécurité et en préservant les gestes barrière)
- un travail d'équipe avec des personnes chargées, par exemple, d'organiser les câbles, de les coupler aux switchs, etc.

Démarrer le TP

Chaque rangée aura besoin d'un Switch et de quelques câbles.

Pour démarrer le TP vous allez devoir importer la machine virtuelle Debian9_Reseau du répertoire /VM-ROOT/VirtualBox. Lorsque vous importez la machine, veuillez choisir l'option qui assure la réinitialisation des adresses MAC. Ouvrez ensuite un terminal dans la machine virtuelle et mettez-vous en root (le mot de passe est : iut)

En bas à droite dans la machine virtuelle vous avez une petite icone avec deux ordinateurs. En faisant un click-droite là-dessus, allez sur les paramétrages réseau. Assurez-vous que la première interface réseau correspond à eth0 et la deuxième, à eth1.

Vos ordinateurs ont deux cartes réseaux et peuvent accueillir deux câbles réseau. Normalement l'interface eth1 correspond au câble haut, tandis que l'interface eth0 correspond au câble bas.

Un rappel des instructions de base : ip, ping est donné à la fin de ce TP. Regardez-le lorsque vous en aurez besoin !

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 : prenez le temps d'assigner des rôles dans l'équipe tel qu'une seule personne travaille sur chaque ordinateur (mais une personne pourra travailler sur plusieurs ordinateurs distincts).

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 l'adresse de votre réseau, écrivez-la sur le tableau en notation CIDR et avec un masque de réseau. Premier arrivé premier servi.
   Quel est votre réseau :

   - En notation CIDR : example : 192.168.3.0/24
   - Avec un masque de réseau : 255.255.255.0

2. Regardez la liste d'options pour la commande ip donnée à la fin du TP. Quelle est la commande qui vous permettra de lister toutes les interfaces disponibles de votre machine ?

   Commande utilisée : ip address show (ip a show, ip add show, etc. marchent également)

   Résultat : Chaque machine devrait avoir les interfaces : lo, eth0, eth1.

3. Et si vous voulez une commande qui ne fait afficher que les interfaces actives ?

   Commande utilisée : ip address show up

   Résultat : Normalement seulement l'interface lo

4. Sur chaque rangée, nous voulons configurer 4 machines, dont les adresses machines sont données ci-dessous.
   Pour chaque machine dans votre rangée, **configurez l'interface eth1** pour qu'elle ait une des adresses machine suivantes (chaque adresse doit apparaître une fois et une fois seulement sur votre rangée), dans votre réseau. N'oubliez pas ensuite d'activer l'interface et de vérifier que la configuration a été correcte.

   44
   135

195
234

Instructions :

ip address add 192.168.3.44/24 dev eth1
ip link set dev eth1 up

5. Utilisez la commande ping (voir la fin du TP !) 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				

Normalement toutes les machines peuvent communiquer entre elles.

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

Les adresses de ces deux sous-réseaux sont :

- Premier sous-réseau : 192.168.3.0/25
- Deuxième sous-réseau : 192.168.3.128/25

Commande à taper sur votre machine (seulement) pour la configurer :

ip address delete 192.168.3.44/24 dev eth1
ip address add 192.168.3.44/25 dev eth1
ip address show up

si l'interface n'est pas activée, alors :
ip link set dev eth1 up

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 ?

   Les machines 135, 195, 234 peuvent encore communiquer mais pas avec la machine 44 car celle-ci est isolée dans son sous-réseau.

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 : 192.168.3.0/26
   - Deuxième sous-réseau : 192.168.3.64/26
   - Troisième sous-réseau : 192.168.3.128/26
   - Quatrième sous-réseau : 192.168.3.192/26

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

   ip address delete 192.168.3.44/25 dev eth1
   ip address add 192.168.3.44/26 dev eth1
   ip address show up

   si l'interface n'est pas activée, alors :
   ip link set dev eth1 up

   Spécifiez quelle machine est désormais dans quel réseau :

   44 dans le premier sous-réseau
   135 dans le troisième sous-réseau
   195,234 dans le quatrième sous-réseau

Exercice 2

1. Nous voulons que la machine 44 puisse communiquer avec les machines 195 et 234. Pour réussir cela, nous allons transformer la machine 135 dans une passerelle. Refaites la configuration de cette machine tel que : sur l'interface eth0 elle aura la dernière adresse IP du réseau de la machine 44 ; et sur l'interface eth1 elle aura la dernière adresse IP du réseau de la machine 195.

Quelles sont les adresses IP configurées ?

eth0 : 192.168.3.62/26
eth1 : 192.168.3.254/26

2. Connectez l'interface eth1 des machines 44, 195 et 234 au Switch de votre groupe (par un câble/machine). Ensuite, connectez les deux interfaces de l'ancienne machine 135 au Switch.

3. Sur l'ancienne machine 135 tapez la commande : `echo 1 > /proc/sys/net/ipv4/ip_forward` (vous verrez au TD2 à quoi cela correspond).

4. Sur la machine 44 configurez une route par défaut via la machine passerelle (interface eth0). Sur la machine 195 configurez une route par défaut via la machine passerelle (interface eth1). Essayez ensuite de configurer sur la machine 234 une route par défaut via la machine passerelle (interface eth0). Est-ce que cela marche ? Pourquoi ?

   Sur 44 :
   ip route add default via 192.168.3.62

   Sur 195 :
   ip route add default via 192.168.3.254

   Sur 234 : message d'erreur qui nous dira que cela sera impossible

   Configurez la passerelle par défaut correcte sur la machine 234.

   Sur 234 :
   ip route add default via 192.168.3.254

5. Sur la machine passerelle, ouvrez Wireshark (regardez la fin de ce TP pour voir comment) et démarrez une capture sur toutes ses interfaces.
   Sur les machines 44, 195 et passerelle tapez premièrement la commande : ip neigh flush. Ensuite, tapez la commande qui permet de faire un ping vers la machine 195. Arrêtez la capture en cliquant sur l'aileron bleu.
   - Trouvez en haut de la fenêtre Wireshark le champ qui nous permet de filtrer les messages capturés par protocole. En utilisant ARP en tant que filtre, trouvez les requêtes et réponses ARP qui ont été faites. Pour chaque requête et réponse relevez les adresses de la source, destination, et cible.

Si aucun cache ARP, normalement 4 trames ARP (4 requêtes/réponses).

La machine 44 a eu besoin de savoir l'@ MAC de la machine passerelle (eth0).
La machine passerelle a eu besoin de savoir l'@MAC de 195.
La machine 195 a eu besoin de l'@ MAC de la machine passerelle (eth1)
La machine passerelle a eu besoin de savoir l'@MAC de 44.

- Isolez maintenant dans la capture les messages ping. Que remarquez vous pour les adresses IP et MAC de chaque message ? Pourquoi ?

  Sur les deux interfaces on aura les adresses IP des machines 44 et 195.
  Sur l'interface eth0, en termes d'adresse MAC, la requête se fait avec l'@ MAC source de la machine 44, et l'@ MAC dest. de la machine passerelle (eth0). Pour la réponse, c'est l'inverse.
  Sur l'interface eth1, en termes d'adresse MAC, la requête se fait avec l'@ MAC source de la machine passerelle (eth1), et l'@ MAC dest. de la machine 195. Pour la réponse, c'est l'inverse.

Exercice 3

1. Nous allons ensuite remettre l'adresse de la machine 44 pour la mettre dans le même réseau qu'on avait à la question 1 de l'exercice 1. Cela devrait également enlever la passerelle par défaut. Vérifiez cela.

   Quelle est l'adresse IP et le réseau (notation CIDR) de la machine 44 ?

   192.168.3.44/24, réseau 192.168.3.0/24

   Quelle est la commande qui vous permet de vérifier le tableau de routage ?

   ip route show

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

   192.168.3.192/26

2. Détachez la machine passerelle du Switch (mettez-la hors-ligne).

3. Maintenant, essayez de faire un ping de la machine 44 vers la machine 195. Quel est le résultat ?

   Le ping par mais ne revient pas.

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

   Le réseau est non-joignable

   Pouvez-vous justifier les deux comportements observés ?

   Les deux machines ne sont plus sur un même réseau.

4. 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.

   filtrage icmp, normalement on le voit.

5. 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 ?

6. Expliquez le comportement que vous avez observé.

   Voir ci-dessus.

Exercice 4

Finalement nous allons essayer de connecter votre machine à l'Internet. Pour ce faire, il faut premièrement trouver l'adresse physique de votre machine.

Allez en dehors de la machine virtuelle, sur votre machine physique. Dans un terminal, tapez l'instruction qui vous permet de visualiser les interfaces de votre machine et les adresses configurées là-dessus. Trouvez, parmi ces adresses, une qui est dans la plage 164.81.118.64/26 pour la salle 104 et 164.81.118.0/26 pour la salle 105.

1. Quelle adresse avez-vous trouvé ?

   A voir sur chaque machine.

2. Rebranchez votre machine au réseau de la salle sur l'interface eth1 (câble haut). Dans la machine virtuelle, configurez l'adresse que vous venez de trouver sur l'interface eth1 de votre machine et enlevez toute autre adresse et configuration.

3. Ajoutez une route par défaut via la passerelle de la salle, notamment : 164.81.118.126 (salle 104) ou 164.81.118.62 (salle 105).

4. Videz la cache ARP de votre machine si elle n'est pas encore vide. Lancez une capture Wireshark sur eth1. Faites un ping et un seul vers l'adresse IP 8.8.8.8, puis arrêtez la capture.

   ip neigh flush pour vider le cache.

5. 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 ?

   La passerelle de la salle.

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

   - L'adresse IP de la machine 8.8.8.8
   - Quelle est la machine dont on indique l'adresse IP ? la vraie destination

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

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

   inconnue car hors réseau

Configurer les interfaces réseaux -- la commande and ip

Nous allons travailler sur Linux. Dans cet environnement la configuration des interfaces réseaux se fait en utilisant la famille de commandes `ip`.

La plupart de ces commandes ne s'utilisent qu'en tant que `root`.

La commande `ip` a la structure générale suivante :

```
ip <options> <objet> <commande> <paramètres>
```

L'utilisation d'options n'est pas obligatoire et les paramètres dépendent de la commande choisie.

Voici par exemple quelques instructions qui sont parmi les plus utilisées.

- `ip address show` : montre toutes les interfaces avec leurs configurations (même si l'interface n'a pas été configurée.
- `ip address show up` : montre seulement les interfaces actives.
- `ip link set <nom d'interface> <up ou down>` : active ou désactive l'interface en question.
  Exemple : `ip link set eth0 up`
- `ip address add <adresse IP/CIDR réseau> dev <nom d'interface>` : configure l'interface nommée à l'adresse IP mentionnée dans le réseau mentionné
  Exemple : `ip address add 192.168.67.2/24 dev eth0`
- `ip address del <adresse IP/CIDR reseau> dev <nom d'interface>` : enlève l'adresse de l'interface mentionnée

De plus, voici les deux commandes qui permettent à réaliser le routage :

- `ip route show` : montre le tableau de routage de la machine
- `ip route add default via <adresse IP de la passerelle>` : réalise une route par défaut via la passerelle
- `ip route add <réseau dst, notation CIDR> via <adresse IP passerelle>` : configure une route spécifique

Et finalement voici comment on peut accéder au cache ARP de la machine :

- `ip neigh` : montre le cache ARP
- `ip neigh flush` : vide le cache ARP

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

Il faut démarrer ce protocole en tant que root, en ligne de commande (tapez wireshark). 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.