IO4 Routage IP et administration réseau – Compléments

Études de cas

À terminer et à rendre la semaine prochaine (par binôme)

1. Plan d'adressage d'une entreprise (à rédiger et à remettre)

L'entreprise *Trucmuche* est en pleine expansion, elle a besoin de rénover l'organisation de son réseau informatique. Vous voilà donc embauché pour réaliser cette tâche…

A ce jour, tous les ordinateurs de l'entreprise sont connectés au sein d'un seul et même **réseau de classe C privé 192.168.10.0**. L'accès à Internet est assuré par un routeur connecté à la fois à ce réseau et à un réseau extérieur.
Un grand nombre de machines sont déjà à la disposition du personnel des 4 grands services de l'entreprise que sont le service « Direction/Comptabilité », le service « Commercial », le service « Après Vente » et le service « Production ».
Cependant, les besoins informatiques évoluant très vite pour la grande majorité des employés, de nouvelles machines sont achetées...
Et c'est ainsi que le nombre limite de machines qu'il est possible de numéroter au sein du réseau actuel est dépassé !...

1. Quel est donc ce nombre limite ?

Il est donc temps d'étudier les différentes possibilités de réorganisation du réseau.

Cas 1 : On souhaite que les machines restent toutes dans le même réseau, connectées à l'aide de commutateurs ou de répéteurs, sans introduire de passerelle autre que le routeur extérieur.

2. Quel numéro de réseau utiliser ? et quel masque ? Quels sont les numéros possibles pour les machines ?

Cas 2 : On s'autorise l'ajout de machines passerelles pour découper le réseau en sous-réseaux. On peut imaginer deux approches différentes (au moins) pour le choix des numéros de réseaux et des masques associés.

3. Pour chacune de ces 2 approches, proposez (« dessinez ») un plan d'adressage complet pour l'entreprise (numéros de réseau, masques et numéros des machines).

Cas 2 bis : Les activités du service « Commercial » justifient une séparation par une passerelle de ses équipements informatiques : ceux concernant la *prospection* et ceux concernant la *vente*. Il en est de même pour le service « Production » avec ses équipements informatiques concernant la *fabrication* et ceux concernant la *gestion des matières premières*.

4. Modifiez en conséquence vos deux plans d'adressages du Cas 2.

2. Passage à la pratique (à remettre dans un répertoire)

Afin de tester le plan d'adressage « théorique » que vous avez proposé à l'exercice précédent (la solution la plus « complexe » des deux), vous allez mettre en œuvre une configuration réseau minimale sous User Mode Linux (UML).

1. Choisissez pour cela 5-6 machines maximum, celles qui vont permettre de valider votre approche (prenez au moins 3 machines sur le réseau fédérateur, dont le routeur extérieur).
2. Créez le script décrivant la configuration réseau sous UML (partez de /net/opt/UML/conf/exemple-reseau). Pour cet exercice vous utiliserez impérativement des machines de type « debian ».
3. Avant de lancer votre script, vous vous assurerez que votre répertoire `~/.cows` est vide ! Si ce n'est pas le cas, soit vous le videz, soit les noms des machines déjà présentes ne doivent pas être les mêmes que ceux présents dans votre nouveau script…
4. Lancez votre script, configurez votre réseau de machines, et testez avec *ifconfig*, *route*, *ping*, etc…
5. Pour sauvegarder votre travail, il faut :
   i. Fermer PROPREMENT toutes les machines virtuelles (commande « *halt* » ou « *shutdown* »),
   ii. Copier les scripts de simulation et les fichiers (« cow »)correspondant à vos machines du répertoire `~/.cows` vers le répertoire de remise : `~/IO4_Remise_Routage`
   iii. Indiquer ce répertoire de remise sur le document papier que vous remettrez.

3. Découverte de l'utilitaire tcpdump

L'utilitaire *tcpdump* permet de tracer les activités réseau en interceptant les paquets entrant et sortant d'une interface réseau. *tcpdump* décode chacun des paquets qu'il intercepte et les affiche sous un format légèrement crypté.

3.1 Installer tcpdump

Pour limiter la taille des machines virtuelles (et donc l'occupation mémoire et disque des machines réelles), l'installation de ces machines est minimale. C'est pourquoi l'utilitaire *tcpdump* n'est pas installé par défaut. Vous devez donc installer le package *tcpdump* sur chacune des machines sur lesquelles vous voudrez l'exécuter.
Pour savoir comment faire, reportez-vous aux notes sur l'utilisation d'UML au département, rubrique « Installer des packages supplémentaires » (/net/exemples/IO4/notes-uml.html).
Vous regarderez en particulier l'option –i pour désigner une autre interface que *eth0*, ou encore les -x et –X qui permettent d'avoir plus d'informations sur les paquets interceptés.
N'hésitez pas à tester un grand nombre d'options lors de vos tests pour mieux comprendre ce qu'il se passe…

3.2 Avant et/ou pendant les tests

Il est important de travailler de façon rigoureuse : « videz » les tables arp de vos machines (voir man arp) chaque fois que vous (re-)commencez un test

3.3 Tests avec Ping

Lancer *tcpdump* sur quelques machines voulues, puis faites quelques *ping* entre des machines d'un même réseau, de réseaux différents, avec les machines sur lesquelles tourne *tcpdump*, etc…
Quelles sont vos conclusions ?

3.4 Tests avec ssh

Même si les conclusions sont plus difficiles à établir avec *ssh* (il y a beaucoup plus de paquets à analyser), refaites les mêmes tests avec *ssh* (créez un compte d'utilisateur normal, parce qu'on ne peut pas faire un ssh vers un compte root pour des raisons de sécurité).
Pouvez-vous dégager quelques conclusions simples ?

3.5 Tests avec le service *daytime*

Ce service (port 13/tcp), lorsqu'il est disponible sur une machine, donne la date et l'heure de la machine. Essayez de vous connecter avec *telnet* sur le port 13 d'une machine linux réelle du département pour voir… Il est possible que ce service soit inactif par défaut. Pour l'activer, dé-commentez la ligne concernée dans le fichier /etc/inetd.conf, et signalez le changement au démon inetd (killall -1 inetd). Essayez alors de vous connecter avec *telnet* sur ce service.
Grâce à *tcpdump*, vous pourrez voir ce qui est échangé, en particulier, utilisez l'option –xX de *tcpdump*.
Que remarquez-vous ?

3.6 D'autres tests

Le protocole ARP (voir explication dans l'article ARP de www.wikipedia.fr si besoin est) entre en jeu quand deux machines d'un réseau local doivent communiquer mais ne connaissent pas encore leurs adresses MAC respectives. Mettez-le en évidence par des expériences avec *tcpdump*, et retrouvez dans les trames transmises les adresses MAC et IP de l'émetteur et du destinataire.

Faire un autre test de votre choix.…

4. Différences Switch / Hub

Vous allez refaire l'ensemble des tests précédents avec *tcpdump*, mais en changeant un peu la configuration réseau. On va remplacer tous les « switch » par des « hub ». Si vous connaissez la différences entre les deux, faites vos pronostics ! Sinon, laissez vous guider par les tests…

1. Fermez toutes les machines virtuelles (*halt*). Le script se termine proprement en sauvegardant vos machines en l'état.
2. Faites une copie de votre script de lancement en remplaçant SWITCH par HUB, puis lancez-le.
3. Refaites tous les tests précédents (au moins *ping*) : quelles sont les différences majeures ?

Indications de réponses

EXO 1

- Cas1 : un réseau privé de classe B, par exemple 172.20.0.0 et masque 255.255.0.0.
- Cas 2 : câblage : un réseau fédérateur avec routeur extérieur et 4 passerelles vers les 4 services, ce qui fait 5 sous-réseaux à numéroter.
    - Solution 1 : 5 réseaux privés de classe C, par ex 192.168.**10**.0, 192.168.**20**.0, 192.168.**30**.0, 192.168.**40**.0, 192.168.**50**.0, avec chacun le masque 255.255.255.0.
    - Solution 2 : 1 seul réseau privé de classe B, par exemple 172.20.0.0, que l'on découpe en 5 sous-réseaux à l'aide du masque 255.255.224.0 : cela donne par ex 172.20.**0**.0, 172.20.**32**.0, 172.20.**64**.0, 172.20.**96**.0, 172.20.**128**.0 (+ pas utilisés : 172.20.**160**.0, 172.20.**192**.0, 172.20.**224**.0)
- Cas 2 bis : on découpe 2 des services en 2.
    - Solution 1 bis : au sein des 2 services, on utilise le masque 255.255.255.128, et donc 2 sous-réseaux 192.168.XX.**0** et 192.168.XX.**128**
    - Solution 2 bis : sein des 2 services, on utilise le masque 255.255.240.0, et donc par exemple pour le sous-réseau 172.20.**64**.0, on le découpe en 2 sous-réseaux 172.20.**64**.0 et 172.20.**80**.0

EXO 3

Ping (voir requête arp seule traverse switch (car broadcast), mais pas la réponse, ni les paquets icmp de ping, requête arp ne doit pas traverser les passerelles par contre)