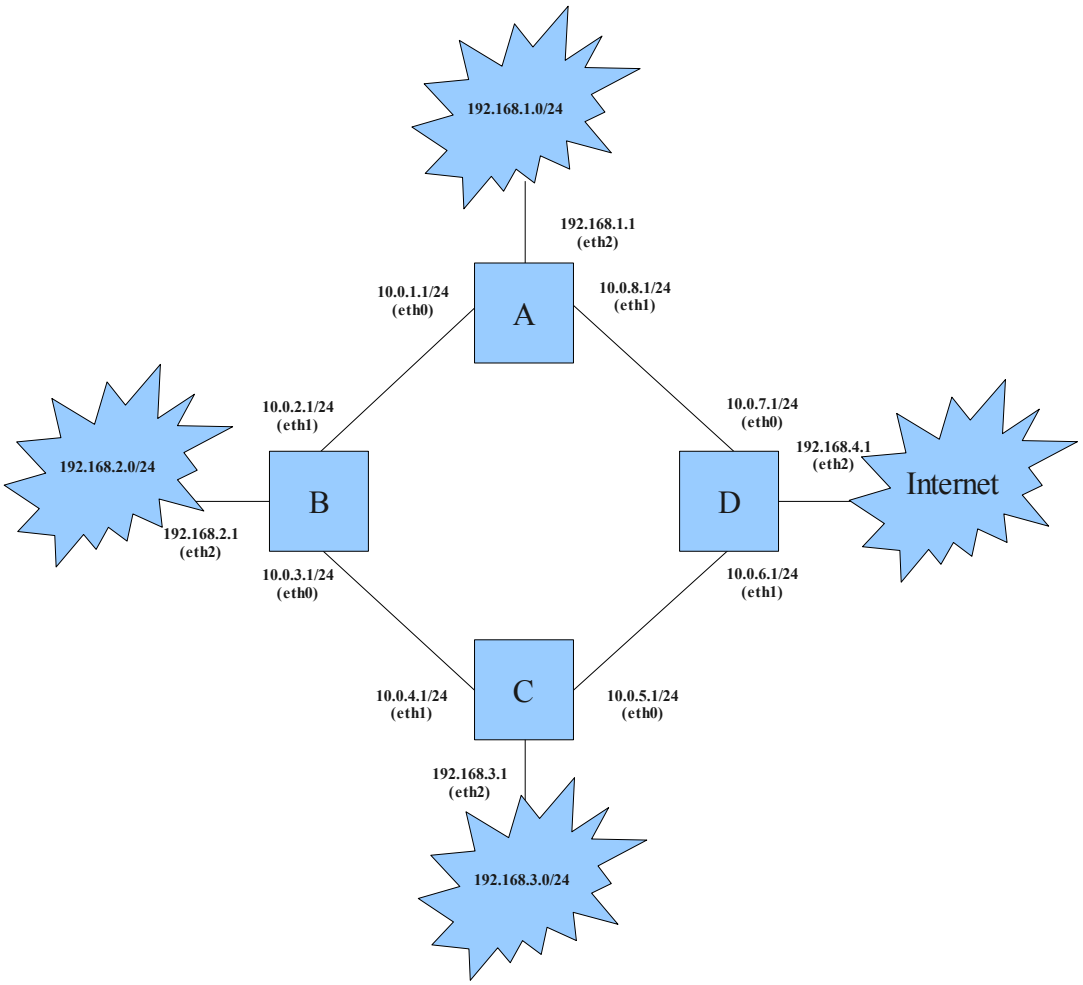
DS MIAGE L3 2008/2009

(Durée 1h30, documents de cours et TD autorisés)

Ex 1 (Routage, 10 pt)

On considère un réseau en anneau de 4 routeurs A, B, C et D, représenté par le schéma suivant : A,B et C servant de relais vers trois sous-réseaux et D servant de passerelle vers Internet.



1. Donner les commandes Linux utilisant “ifconfig” qui permettent de configurer les IPs de la machine A.

On suppose maintenant que toutes les interfaces des machines A, B, C et D sont correctement configurées.

2. A l'aide de la commande Linux “route”, écrire une règle de routage permettant à la machine A de communiquer avec C. Faire de même pour que C communique avec A. Quel choix de *gateways* faites-vous dans ces deux cas ? Justifier.

On suppose maintenant que les tables de routage des machines A, B, C et D sont bien configurées pour communiquer entre elles. On considère la machine C' du sous-réseau 192.168.3.0/24.

3. Ecrire pour la machine C' une règle de routage lui permettant de contacter les machines du sous-réseau 192.168.1.0/24.
4. Ecrire une régle de routage permettant à C' d'accéder à Internet.

Ex 2 (IP, 3 pt)

1. Soit le réseau 192.168.1.0/24. Combien de machines peut-on numéroter dans un tel réseau ? Donner le masque. Donner la plage d'adresses IP pour les machines de ce réseau.
2. Mêmes questions avec 192.168.1.128/26.

Ex 3 (CRC, 5 pt)

Un protocole de communication utilise la méthode CRC pour la détection d'erreurs avec le polynôme générateur : $x^3 + x + 1$. On souhaite transmettre le message B7 (en hexadécimal).

1. Convertir ce message au format binaire.
2. Calculer le bloc de contrôle d'erreurs CRC pour ce message. Donner le résultat au format binaire.

On prendra soin de détailler les calculs.

Ex 4 (ARP, 2 pt)

1. Expliquer brièvement à quoi sert le protocole ARP. (3L max)
2. Qu'est-ce que l'ARP spoofing ? (3L max)

Correction DS 2009

Ex 1 (Routage, 10 pt)

1. On configure les trois IPs de la machine A (masque 24 bits).

   root@A$ ifconfig eth0 10.0.1.1 netmask 255.255.255.0
   root@A$ ifconfig eth1 10.0.8.1 netmask 255.255.255.0
   root@A$ ifconfig eth2 192.168.1.1 netmask 255.255.255.0

2. On suppose maintenant que toutes les interfaces des machines A, B, C et D sont correctement configurées. On écrit une règle de routage pour que A communique avec C et réciproquement. On choisit dans un cas de prendre B comme passerelle et dans l'autre cas de prendre D, afin de répartir le traffic.

   root@A$ route add -host 10.0.4.1 gw 10.0.2.1 dev eth0
   root@C$ route add -host 10.0.8.1 gw 10.0.6.1 dev eth0

3. On suppose maintenant que les tables de routage des machines A, B, C et D sont bien configurées pour communiquer entre elles. On considère la machine C' du sous-réseau 192.168.3.0/24. On écrit pour la machine C' une règle de routage lui permettant de contacter les machines du sous-réseau 192.168.1.0/24.

   root@C'$ route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.3.1

   La règle suivante répondait aussi à la question.

4. On écrit une règle de routage (par défaut) permettant à C' d'accéder à Internet.

   root@C'$ route add default gw 192.168.3.1

Errata : Les adresses IP des machines A, B, C et D pour les interfaces eth0 et eth1 ne sont pas bien choisies, car elles ne correspondent pas à des sous-réseaux de 24 bits comme le schéma le laisse supposer. Toutefois, cela ne remet pas en cause l'écriture des règles de routage demandées.

Ex 2 (IP, 3 pt)

1. Soit le réseau 192.168.1.0/24. Combien de machines peut-on numéroter dans un tel réseau ? Donner le masque. Donner la plage d'adresses IP pour les machines de ce réseau.

   Avec un masque 24 bits (adresse IP sur 32 bits), on dispose de 8 bits pour numéroter les machines soit $2^8 = 256$ possibiltés, auxquelles il faut retrancher l'adresse .0 et .255, ce qui nous fait un total de 254 machines. Masque : 255.255.255.0. Plage : 192.168.1.0 - 192.168.1.255.

2. Mêmes questions avec 192.168.1.128/26.

   Pour un masque 26 bits, on dispose de 6 bits, soit 64-2=62 possibilités pour numéroter des machines. Masque : 255.255.255.X avec X = (1100 000)2 = 128 + 64 = 192. Plage : 192.168.1.128 - 192.168.1.Y avec Y = 128 + (64 - 1) = 191.

Ex 3 (CRC, 5 pt)

Un protocole de communication utilise la méthode CRC pour la détection d'erreurs avec le polynôme générateur : $x^3 + x + 1$. On souhaite transmettre le message B7 (en hexadécimal).

1. Convertir ce message au format binaire.

   Un chiffre hexadécimal est codé sur 4 bits, soit 16 valeurs notée de 0 et 9, puis de A à F.
   ... ; $7_{16} = 7_{10} = 0111_2$; ... ; $A_{16} = 10_{10} = 1010_2$; $B_{16} = 10_{10} = 1010_2$; $B_{16} = 11_{10} = 1011_{2\ ;\ ...}$
   Donc $(B7)_{16} = (1011\ 0111)_2$

2. Calculer le bloc de contrôle d'erreurs CRC pour ce message. Donner le résultat au format binaire. On prendra soin de détailler les calculs.

   Le polynôme générateur est de degrès 3, donc le reste que l'on va calculer est au plus de degrès 2, donc la clé sera codé sur 3 bits. Après calcul, on trouve C(X) = X ; donc la clé est 010.

Ex 4 (ARP, 2 pt)

1. Expliquer brièvement à quoi sert le protocole ARP.
   cf. Cours.

2. Qu'est-ce que l'ARP spoofing ?

   Soit P la machine du pirate et X la machine piratée souhaitant communiquer avec Y. L'ARP spoofing est une “technique de piratage” basée sur le fonctionnement du protocole ARP qui permet à la machine pirate P de recevoir le traffic que X souhaite transmettre à Y. Le spoofing consiste à polluer le cache ARP de la machine X : pour cela le pirate P doit envoyer de manière agressive à X des réponses ARP indiquant que l'adresse IP de Y correspond à l'adresse MAC du pirate P (qui se substitue à l'adresse MAC de Y dans le cache ARP de X). Si le pirate fait de même pour Y vis-à-vis de X, il peut même intercepter le traffic réseau entre X et Y de manière transparente pour ces deux machines ; pour cela, il doit en plus router les messages de X vers Y et réciproquement.