

DS MIAGE L3 2011/2012

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

Ex 1 (Hamming & CRC, 8 pt)

On souhaite envoyer le mot 0101001 en détectant d'éventuelles erreurs de transmission.

1. Quel est le code de Hamming (11,7) correspondant à ce mot ?
2. Quel est la clé CRC si l'on prend $x^3 + x^2 + x$ comme polynôme générateur ?

Nota Bene : On prendra soin de détailler les calculs.

Ex 3 (Adressage en IPV4 avec CIDR, 5 pt)

Avant l'introduction de CIDR¹ dans IPV4, les réseaux utilisaient simplement une approche par classe (A, B ou C). A l'inverse, CIDR (*Classless Inter Domain Routing*) est une approche sans classe. On ne considère plus une adresse comme appartenant implicitement à l'une des trois classes A, B ou C. En CIDR, on associe explicitement à toute adresse de réseau IP un masque qui définit le préfixe qui caractérise le réseau auquel correspond cette adresse. Les adresses de réseaux sont donc maintenant toujours utilisées avec leur préfixe qui peut être de taille arbitraire (par exemple /8, /17, /21).

1. Considérons l'adresse CIDR d'un réseau qui serait 193.53.32.0/20. Quelle serait le nombre d'hôtes que comporterait ce réseau ? Quel est le masque de ce réseau ? Quelle est l'adresse la plus petite utilisable pour un hôte et quelle est la plus grande ?
2. Une entreprise s'adresse à un FAI (Fournisseur d'Accès Internet) pour obtenir 800 adresses. Que doit faire le FAI dans l'adressage par classes pour satisfaire son client et avec quels inconvénients ?

Nous supposons que le FAI a reçu pour exercer son activité le bloc d'adresses 202.0.64.0/18 avec lequel il a constitué son réseau. On suppose qu'au moment de la demande la première adresse réseau qui est libre est 202.0.70.0.

3. Que fait le FAI dans l'approche CIDR pour satisfaire un client qui demande 800 adresses ?
4. En résumé montrez en quoi CIDR constitue une amélioration majeure de l'adressage IPV4 par rapport à l'approche par classe.

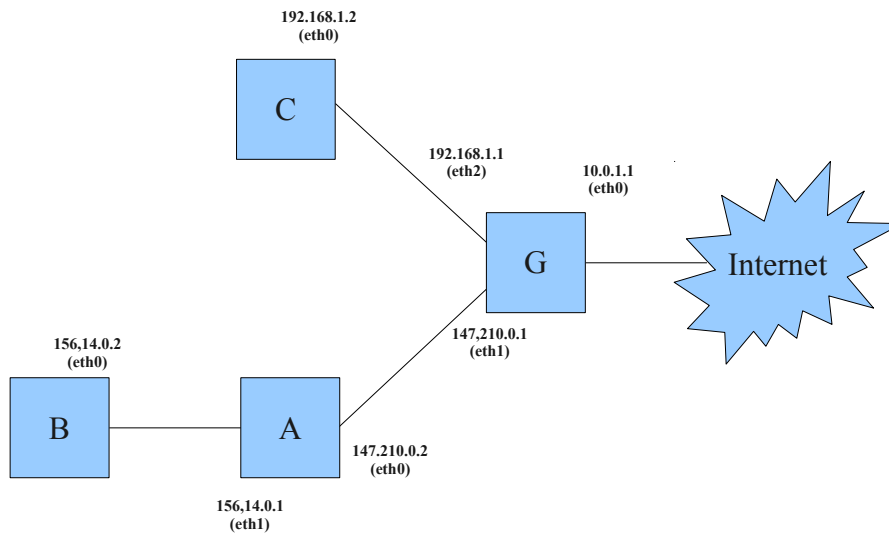
¹ Nous avons étudié CIDR en cours sans le nommer.

Ex 4 (cours, 2 pt)

1. Sur l'internet, deux machines à deux endroits différents peuvent elles posséder la même adresse IPv4 ? Si oui, à quelle condition ?
2. Dans le même réseau IPv4, deux machines différentes peuvent elles posséder la même adresse IPv4 à deux moments différents ? Chercher un contexte d'utilisation.

Ex 5 (Administration, 5 pt)

On souhaite mettre en place un réseau domestique connecté à Internet par la passerelle G et organisé selon le schéma ci-dessous. On supposera que tous les sous-réseaux sont en /24.



On suppose que les IPs sont bien configurées. On demande de lister les commandes Linux nécessaires pour réaliser les tâches suivantes :

1. Configurez les tables de routage pour que toute les machines puissent communiquer ensemble et avec Internet.

On suppose que le firewall est configuré sur G avec une politique par défaut à DROP.

2. Autorisez la machine B à se connecter au web.
3. Autorisez la machine B à se connecter à la machine C par SSH (port 22).
4. On suppose que la machine C héberge un serveur applicatif dédié aux besoins d'une entreprise. Ce serveur fonctionne de la manière suivante : un client se connecte tout d'abord sur le port tcp/8888 du serveur et ensuite le serveur ouvre une connection sur le port tcp/9999 de la machine cliente. Configurez le firewall pour qu'il permette ce serveur de fonctionner normalement. Critiquez votre solution.

Correction

Ex 1 (Hamming & CRC, 8 pt)

On souhaite envoyer le mot 0101001 en détectant d'éventuelles erreurs de transmission.

1. Quel est le code de Hamming (11,7) correspondant à ce mot ? (4pt)

Après calcul on trouve, **10001011001**.

2. Quel est la clé CRC si l'on prend $x^3 + x^2 + x$ comme polynôme générateur ?

$G(x) = x^3 + x^2 + x$; $B(x) = x^5 + x^3 + 1$; $B(x).x^3 = x^8 + x^6 + x^3$; $B(x).x^3 / G(x)$ donne $Q(x) = x^5 + x^4 + x^3 + x$ avec $C(x) = x^2$ comme reste. Au final la clé binaire est **100**.

Ex 3 (Adressage en IPV4 avec CIDR, 5 pt)

Avant l'introduction de CIDR² dans IPV4, les réseaux utilisaient simplement une approche par classe (A, B ou C). A l'inverse, CIDR (*Classless Inter Domain Routing*) est une approche sans classe. On ne considère plus une adresse comme appartenant implicitement à l'une des trois classes A, B ou C. En CIDR, on associe explicitement à toute adresse de réseau IP un masque qui définit le préfixe qui caractérise le réseau auquel correspond cette adresse. Les adresses de réseaux sont donc maintenant toujours utilisées avec leur préfixe qui peut être de taille arbitraire (par exemple /8, /17, /21).

1. Considérons l'adresse CIDR d'un réseau qui serait 193.53.32.0/20. Quelle serait le nombre d'hôtes que comporterait ce réseau ? Quel est le masque de ce réseau ? Quelle est l'adresse la plus petite utilisable pour un hôte et quelle est la plus grande ?

Il y a 20 bits réservés pour la partie réseau et donc 12 bits restants pour la partie hôte. Le nombre max d'hôtes dans ce réseau est alors $2^{12} = 4096$. Le masque s'écrit donc en binaire 11111111.11111111.11110000.00000000 (avec 12 bits de poids faible à 0), ce qui se traduit en décimal par 255.255.240.0. L'adresse minimale est l'adresse du réseau 193.53.32.0 ; l'adresse maximale (ou de broadcast) est telle que les 12 bits de poids faible sont mis à 1, ce qui donne 193.53.47.255 car 32 en binaire s'écrit 0010 0000 et 0010 1111 donne 47 en décimal.

2. Une entreprise s'adresse à un FAI (Fournisseur d'Accès Internet) pour obtenir 800 adresses. Que doit faire le FAI dans l'adressage par classes pour satisfaire son client et avec quels inconvénients ?

La FAI doit choisir une classe suffisamment grande pour contenir les 800 adresses. La classe C contient au plus $2^8 = 256$ machines ; elle est donc trop petite. Il faut donc choisir la classe B, qui contient au plus $2^{16} = 65536$ machines ; mais il y aura beaucoup d'adresses inutilisées !

Nous supposons que le FAI a reçu pour exercer son activité le bloc d'adresses 202.0.64.0/18 avec lequel il a constitué son réseau. On suppose qu'au moment de la demande la première adresse réseau qui est libre est 202.0.70.0.

3. Que fait le FAI dans l'approche CIDR pour satisfaire un client qui demande 800 adresses ?

La taille optimale du réseau est la puissance de 2 immédiatement supérieure à 800, c'est-à-dire $2^{10} = 1024$. Il faut donc réserver 10 bits pour la partie hôte et donc $32-10=22$ bits pour la partie réseau.

2 Nous avons étudié CIDR en cours sans le nommer.

On serait tenter de répondre que le FAI va fournir le sous-réseau 202.0.70.0/22, mais c'est une erreur ! En effet, il faut chercher une adresse réseau de la forme $A_{32}=(R_{22}|H_{10})$ avec $R_{22}=rrr\dots r$ les 22 bits codant la partie réseau et $H_{10}=hhh\dots h$ les 10 bits codant la partie hôte. Par définition, $H^{10} = 000\dots 0$ et il faut trouver R_{22} tel que $A_{32} \geq 202.0.70.0$. Un petit raisonnement rapide nous montre qu'il faut chercher le réseau $202.0.x.0 \geq 202.0.70.0$ respectant les contraintes énoncées. Soit (0100 01|10) la décomposition binaire de 70. Il en résulte qu'il faut choisir $x = 0100\ 10|00$ en binaire, c'est-à-dire $x = 72$. En conclusion, il fallait répondre que le FAI donne le sous-réseau 202.0.72.0.

Nota Bene : Ce n'était pas un exercice si facile qu'il n'y paraît ! [bonus +1 pt]

- En résumé montrez en quoi CIDR constitue une amélioration majeure de l'adressage IPv4 par rapport à l'approche par classe.

Il faut remarquer que CIDR permet d'ajuster la taille du réseau au plus près de la demande cliente. Pour un client demandant un réseau de taille 800 machines, l'approche par classe nécessite un réseau de taille 65536 contre un réseau de taille 1024 dans l'approche CIDR, soit 98.8% d'adresse inutilisée dans le premier cas contre 21.9% dans le second.

Ex 4 (cours, 2 pt)

- Sur l'internet, deux machines à deux endroits différents peuvent elles posséder la même adresse IPv4 ? Si oui, à quelle condition ?

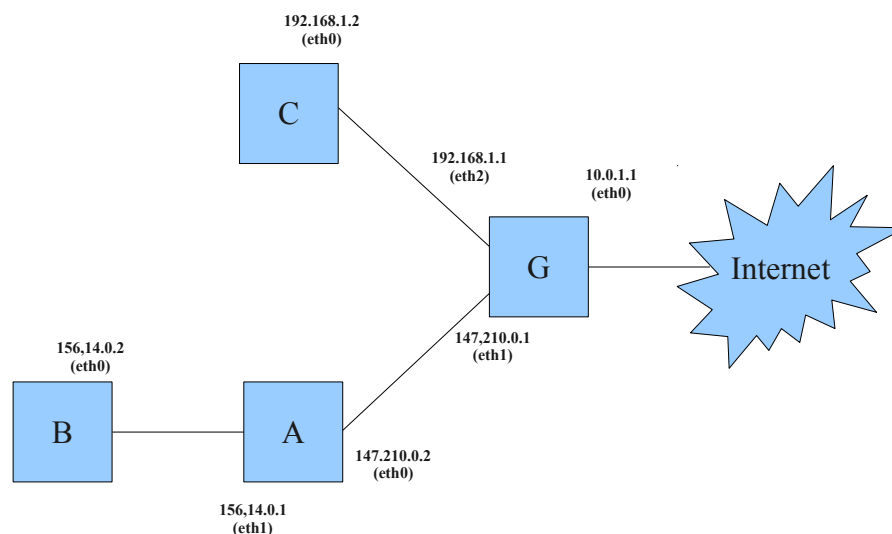
cf. cours

- Dans le même réseau IPv4, deux machines différentes peuvent elles posséder la même adresse IPv4 à deux moments différents ? Chercher un contexte d'utilisation.

cf. cours

Ex 5 (Administration, 6 pt)

On souhaite mettre en place un réseau domestique connecté à Internet par la passerelle G et organisé selon le schéma ci-dessous. On supposera que tous les sous-réseaux sont en /24.



On suppose que les IPs sont bien configurées. On demande de lister les commandes Linux nécessaires pour réaliser les tâches suivantes :

1. Configurez les tables de routage pour que toute les machines puissent communiquer ensemble et avec Internet.

```
A$ route add default gw 147.210.0.1
B$ route add default gw 156.14.0.1
C$ route add default gw 192.168.1.1
G$ route add -net 156.14.0.0 netmask 255.255.255.0 gw 147.210.0.2
G$ route add default gw @GW      (avec @GW l'adresse de la passerelle Internet)
```

Il faut aussi penser à activer le mode routeur pour A et G :

```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

On suppose que le firewall est configuré sur G avec une politique par défaut à DROP.

2. Autorisez la machine B à se connecter au web.

```
G$ iptables -A FORWARD -s 156.14.0.2 -p tcp --dport 80 -j ACCEPT
G$ iptables -A FORWARD -d 156.14.0.2 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

3. Autorisez la machine B à se connecter à la machine C par SSH (port 22).

```
G$ iptables -A FORWARD -s 156.14.0.2 -d 192.168.1.2 -p tcp --dport 22 -j ACCEPT
G$ iptables -A FORWARD -d 156.14.0.2 -s 192.168.1.2 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

4. On suppose que la machine C héberge un serveur applicatif dédié aux besoins d'une entreprise. Ce serveur fonctionne de la manière suivante : un client se connecte tout d'abord sur le port tcp/8888 du serveur et ensuite le serveur ouvre une connection sur le port tcp/9999 de la machine cliente. Configurez le firewall pour qu'il permette ce serveur de fonctionner normalement. Critiquez votre solution.

```
G$ iptables -A FORWARD -d 192.168.1.2 -p tcp --dport 8888 -j ACCEPT
G$ iptables -A FORWARD -s 192.168.1.2 -p tcp --sport 8888 -m state --state ESTABLISHED -j ACCEPT
G$ iptables -A FORWARD -s 192.168.1.2 -p tcp --dport 9999 -j ACCEPT
G$ iptables -A FORWARD -d 192.168.1.2 -p tcp --sport 9999 -m state --state ESTABLISHED -j ACCEPT
```

Le firewall tel qu'il est configuré ne permet pas de voir que les deux connexions sont reliées. Comme dans le cas du FTP, il faudrait utiliser l'état RELATED, mais cela n'a pas de sens pour un protocole défini par l'utilisateur. [bonus +1 pt]