

 <b>BORDEAUX 1</b> Sciences Technologiques <b>DISVE</b> Licence	<b>ANNEE UNIVERSITAIRE 2009/2010</b> SESSION 1 DE PRINTEMPS  <b>ETAPE : MIAGE L3</b> <b>UE : INF157</b> <b>Epreuve : Réseaux informatiques</b> <b>Date : 12/05/2010</b> <b>Heure : 11h00</b> <b>Durée : 1h30</b> Documents : Tous documents de cours et de TP autorisés. Epreuve de M <sup>r</sup> Esnard Aurélien	 Département <b>D L</b> Licence
--	---	---

**Nota Bene :** Le barème est donné à titre indicatif.

### Exercice 1 (Réseau et sous-réseaux, 4 pt)

*Exercice extrait de l'examen réseau 2007-2008 du Master 2 CCI de l'Université d'Orléans.*

Vous devez gérer un réseau d'entreprise qui relie 3 bâtiments : le bâtiment B1 qui regroupe environ 1200 machines, le bâtiment B2 avec 400 machines et le bâtiment B3 avec 800 machines.

1. Si vous devez demander un bloc d'adresses IP contigu, quelle est la longueur maximale du masque réseau que vous pouvez avoir pour réussir cet adressage ?
2. Supposez que le bloc que vous recevez commence à l'adresse IP 133.239.96.0. Quel est l'adresse IP la plus élevée que vous pouvez attribuer dans votre réseau ?
3. Réalisez le découpage de cette plage d'adresses en trois sous-réseaux. Donner, pour chaque bâtiment, le numéro du réseau, l'adresse de la première machine, l'adresse de la dernière machine et l'adresse de diffusion.

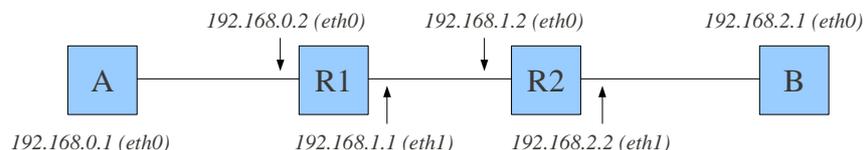
### Exercice 2 (Code de Hamming, 4 pt)

On considère le code de Hamming (11,7) étudié en cours. On détaillera le calcul.

1. Quel est le code de Hamming correspondant au mot 0100111 ?
2. Quel est le message correspondant au code 01010110011 ? Y a-t-il un erreur ? Si oui la corriger.

### Exercice 3 (Routage et Firewall, 6 pt)

On considère le réseau suivant composé de deux machines A et B et de deux routeurs R1 et R2.



1. Configurez les tables de routage de A et B en utilisant la commande « route ».
2. On suppose maintenant que la route par défaut de R1 est R2 et réciproquement. Donnez les commandes nécessaires pour effectuer ce routage.

3. Que se passe-t-il lorsque A effectue un ping vers une adresse invalide, par exemple 192.168.3.1 ?  
Détaillez votre réponse. Si nécessaire proposer une correction à la configuration précédente.
4. On suppose maintenant que la machine B héberge un serveur SSH (protocole TCP, port 22) dont la machine A est cliente. A l'aide de la commande « iptables », mettre en place un firewall sur les machines A et B autorisant uniquement l'utilisation du service SSH.

#### Exercice 4 (Analyse de trames, 4 pt)

A l'aide d'un outil comme Tcpdump, nous avons capturé les trames suivantes.

No.	Time	Source	Destination	Protocol	Info
2	5.002810	a2:00:00:00:03:00	a2:00:00:00:01:00	ARP	Who has 192.168.0.2? Tell 192.168.0.1
3	5.003349	a2:00:00:00:01:00	a2:00:00:00:03:00	ARP	192.168.0.2 is at a2:00:00:00:01:00
4	7.037822	192.168.0.2	192.168.0.1	TCP	59580 > daytime [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=88626 TSER=0 WS=3
5	7.037847	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=88585 TSER=88626 WS=3
6	7.039340	192.168.0.2	192.168.0.1	TCP	59580 > daytime [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=88626 TSER=88585
7	7.051655	192.168.0.1	192.168.0.2	DAYTIME	DAYTIME Response
8	7.051791	192.168.0.2	192.168.0.1	TCP	59580 > daytime [ACK] Seq=1 Ack=27 Win=5840 Len=0 TSV=88631 TSER=88585
9	7.051802	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [FIN, ACK] Seq=27 Ack=1 Win=5792 Len=0 TSV=88585 TSER=88631
10	7.053165	192.168.0.2	192.168.0.1	TCP	59580 > daytime [FIN, ACK] Seq=1 Ack=28 Win=5840 Len=0 TSV=88631 TSER=88585
11	7.053172	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [ACK] Seq=28 Ack=2 Win=5792 Len=0 TSV=88585 TSER=88631

A quoi correspond selon vous le trafic capturé ? Détaillez brièvement chacune des trames en s'appuyant sur un schéma. (15L max.)

#### Exercice 5 (Cours, 2 pt)

Décrivez la valeur ajoutée d'IP dans l'empilement des couches réseaux. (5L max.)

# Correction

## Exercice 1 (Réseau et sous-réseaux, 4 pt)

Vous devez gérer un réseau d'entreprise qui relie 3 bâtiments : le bâtiment B1 qui regroupe environ 1200 machines, le bâtiment B2 avec 400 machines et le bâtiment B3 avec 800 machines.

1. Si vous devez demander un bloc d'adresses IP contigu, quelle est la longueur maximale du masque réseau que vous pouvez avoir pour réussir cet adressage ?

*Au total, on dénombre  $1200+400+800 = 2400$  machines. Il faut donc 12 bits car  $2^{12} = 4096 > 2400$ . Par conséquent, le masque de réseau a une longueur maximale de  $32-12 = 20$  bits. Le masque est alors : 255.255.240.0.*

*Cependant, si on souhaite obtenir 3 sous-réseaux de tailles identiques, il faut alors 13 bits (11 bits par sous-réseau + 2 bits pour coder les 3 sous-réseaux). Dans ce cas, il faut un masque de réseau de longueur 19 bits, avec 255.255.224.0 comme masque.*

2. Supposez que le bloc que vous recevez commence à l'adresse IP 133.239.96.0. Quel est l'adresse IP la plus élevée que vous pouvez attribuer dans votre réseau ?

*96 s'écrit en binaire  $(0110\ 0000)_2$ . Etant donné un masque de réseau /20, l'IP la plus haute va s'écrire  $133.239.(0110\ 1111)_2.(1111\ 1111)_2 = 133.239.111.255$ .*

*Pour un masque /19, l'IP la plus haute sera alors  $133.239.(0111\ 1111)_2.(1111\ 1111)_2 = 133.239.127.255$ .*

3. Réalisez le découpage de cette plage d'adresses en trois sous-réseaux. Donner, pour chaque bâtiment, le numéro du réseau, l'adresse de la première machine, l'adresse de la dernière machine et l'adresse de diffusion.

*Pour faire au plus simple, on décide de construire 3 sous-réseaux identiques dans le réseau 133.239.96.0/19 (pas possible dans /20). Pour coder 3 sous-réseaux, on utilise 2 bits, ce qui permet d'obtenir au plus 4 sous-réseaux identiques comportant chacun  $2^{11} = 2048$  adresses (masque de sous-réseau en /21). Au final, on a les plages suivantes :*

- B1 (Rx 00) = 133.239.96.0 – 133.239.103.255 ;
- B2 (Rx 01) = 133.239.104.0 – 133.239.111.255 ;
- B3 (Rx 10) = 133.239.112.0 – 133.239.119.255.

*Une autre solution possible avec un masque de réseau en /20 et des sous-réseaux de tailles variables (VLSM). Pour coder 3 ces sous-réseaux, on utilise typiquement 2 bits, ce qui permet d'obtenir au plus 4 sous-réseaux identiques comportant chacun  $2^{10} = 1024$  adresses (masque de sous-réseau de longueur 22 bits). Cela convient parfaitement pour B2 et B3, mais pas pour B1 qui a besoin de plus d'adresses. Nous allons donc fusionner deux sous-réseaux pour B1, ce qui permet d'obtenir un total 2048 adresses  $> 1200$ . Au final, on se propose d'utiliser les sous-réseaux numéro 00 et 01 pour B1; le sous-réseau 10 pour B2 et le sous-réseau 11 pour B3. En résumé : B1, réseau d'adresse 133.239.(0110 0000)<sub>2</sub> .0 avec un masque de sous-réseau de 21 bits, autorisant 2048 adresses comprises entre 133.239.96.0 et 133.239.103.255 ; B2, réseau d'adresse 133.239.(0110 1000)<sub>2</sub> .0 avec un masque de sous-réseau de 22 bits, autorisant 1024 adresses comprises entre 133.239.104.0 et 133.239.107.255 ; B3, réseau d'adresse 133.239.*

(0110 1100)2 .0 avec un masque de sous-réseau de 22 bits, autorisant 1024 adresses comprises entre 133.239.108.0 et 133.239.111.255. D'autres solutions sont encore envisageables.

*Nota Bene* : Pour plus d'info sur les sous-réseaux de tailles variables, cf. VLSM (Variable Length Subnet Masking).  
<http://www.iprezo.org/index.php?page=vlsm>

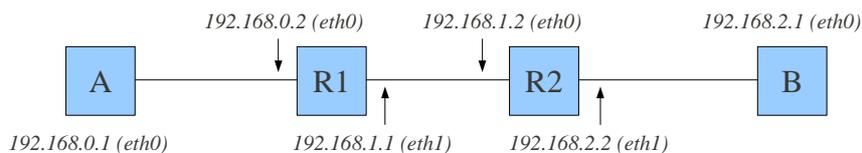
### Exercice 2 (Code de Hamming, 4 pt)

On considère le code de Hamming (11,7) étudié en cours. On détaillera le calcul.

1. Quel est le code de Hamming correspondant au mot 0100111 ?  
*Le code de Hamming de ce mot est 10011001111. Justifiez les calculs.*
2. Quel est le message correspondant au code 01010110011 ? Y a-t-il un erreur ? Si oui la corriger.  
*Le message est 0011011. Les bits de contrôle P2 et P3 sont faux ! L'erreur se trouve donc sur le 6ème bit (car P2 contrôle  $2^1$  et P3 contrôle  $2^2$ ,  $2 + 4 = 6$ ), c'est-à-dire D3 (et non D6). On corrige : le mot est alors 0001011.*

### Exercice 3 (Routage et Firewall, 6 pt)

On considère le réseau suivant composé de deux machines A et B et de deux routeurs R1 et R2.



1. Configurez les tables de routage de A et B en utilisant la commande « route ».  
*A\$ route add default gw 192.168.0.2*  
*B\$ route add default gw 192.168.2.2*
2. On suppose maintenant que la route par défaut de R1 est R2 et réciproquement. Donnez les commandes nécessaires pour effectuer ce routage.  
*R1\$ route add default gw 192.168.1.2*  
*R2\$ route add default gw 192.168.1.1*
3. Que se passe-t-il lorsque A effectue un ping vers une adresse invalide, par exemple 192.168.3.1 ?  
Détaillez votre réponse. Si nécessaire proposer une correction à la configuration précédente.  
*A n'a pas de route spécifique pour 192.168.3.1 ; il utilise donc sa route par défaut et transmet le message ICMP (ping) à R1. R1 procède de même et transmet le message à R2 en suivant sa route par défaut. De la même façon, R2 transmet le message à R1 en suivant sa route par défaut, et ainsi de suite ! Le message va donc « boucler » entre R1 et R2. Cette boucle serait infinie sans le mécanisme du Time-To-Leave (TTL) utilisé par IP (cf. cours). Pour corriger ce problème, il convient d'utiliser des routes spécifiques et non des routes par défaut pour les routeurs R1 et R2 :  
*R1\$ route add -net 192.168.2.0/24 gw 192.168.1.2**

*R2\$ route add -net 192.168.0.0/24 gw 192.168.1.1*

4. On suppose maintenant que la machine B héberge un serveur SSH (protocole TCP, port 22) dont la machine A est cliente. A l'aide de la commande « iptables », mettre en place un firewall sur les machines A et B autorisant uniquement l'utilisation du service SSH.

*A\$ iptables -A OUTPUT -d 192.168.2.1 -p tcp --dport 22 -j ACCEPT*

*A\$ iptables -A INPUT -s 192.168.2.1 -p tcp --sport 22 -m state -- state ESTABLISHED -j ACCEPT*

*A\$ iptables -P INPUT DROP ; iptables -P OUTPUT DROP ; iptables -P FORWARD DROP*

*B\$ iptables -A INPUT -s 192.168.0.1 -p tcp --dport 22 -j ACCEPT*

*B\$ iptables -A OUTPUT -d 192.168.2.1 -p tcp --sport 22 -m state -- state ESTABLISHED -j ACCEPT*

*B\$ iptables -P INPUT DROP ; iptables -P OUTPUT DROP ; iptables -P FORWARD DROP*

#### Exercice 4 (Analyse de trames, 4 pt)

A l'aide d'un outil comme Tcpdump, nous avons capturé les trames suivantes.

No.	Time	Source	Destination	Protocol	Info
2	5.002810	a2:00:00:00:03:00	a2:00:00:00:01:00	ARP	Who has 192.168.0.2? Tell 192.168.0.1
3	5.003349	a2:00:00:00:01:00	a2:00:00:00:03:00	ARP	192.168.0.2 is at a2:00:00:00:01:00
4	7.037822	192.168.0.2	192.168.0.1	TCP	59580 > daytime [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=88626 TSER=0 WS=3
5	7.037847	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=88585 TSER=88626 WS=3
6	7.039340	192.168.0.2	192.168.0.1	TCP	59580 > daytime [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=88626 TSER=88585
7	7.051655	192.168.0.1	192.168.0.2	DAYTIME	DAYTIME Response
8	7.051791	192.168.0.2	192.168.0.1	TCP	59580 > daytime [ACK] Seq=1 Ack=27 Win=5840 Len=0 TSV=88631 TSER=88585
9	7.051802	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [FIN, ACK] Seq=27 Ack=1 Win=5792 Len=0 TSV=88585 TSER=88631
10	7.053165	192.168.0.2	192.168.0.1	TCP	59580 > daytime [FIN, ACK] Seq=1 Ack=28 Win=5840 Len=0 TSV=88631 TSER=88585
11	7.053172	192.168.0.1	192.168.0.2	TCP	daytime > 59580 [ACK] Seq=28 Ack=2 Win=5792 Len=0 TSV=88585 TSER=88631

A quoi correspond selon vous le trafic capturé ? Détaillez brièvement chacune des trames en s'appuyant sur un schéma. (15L max.)

- *Dans la séquence capturée, la machine 192.168.0.2 (client) se connecte au service daytime de la machine 192.168.0.1 (serveur), qui lui envoie une réponse, a priori la date et l'heure (trame n°7).*
- *Plus précisément, on observe dans les trames n° 2 et 3 une requête ARP « who has » du serveur qui cherche l'adresse MAC du client.*
- *Puis les trames n° 4, 5 et 6 décrivent l'établissement d'une connexion TCP/IP de 192.168.0.2:59580 vers 192.168.0.1:13 (n° port standard du service daytime). Il s'agit de la classique poignée de main SYN → SYN+ACK → ACK.*
- *Une fois la connexion établie, le serveur Daytime envoie directement un message au client (trame n° 7), message qui est ensuite acquité (ACK) par le client avec la trame n° 8.*
- *Puis le serveur initie la terminaison de la connexion TCP/IP (trames n° 9, 10, 11) avec la séquence classique FIN → FIN+ACK → ACK.*

#### Exercice 5 (Cours, 2 pt)

Décrivez la valeur ajoutée d'IP dans l'empilement des couches réseaux. (5L max.)

*Cf. Cours.*