DISVE Licence	**ANNEE UNIVERSITAIRE 20012/2013** **SESSION 1** **ETAPE : MIAGE L3** **UE : J1IN6026** **Epreuve : Réseaux informatiques** **Date :** 30/04/2013 **Heure :** 11h00 **Durée :** 1h30 Documents : Tous les documents sont interdits. Epreuve de Mr Esnard Aurélien	

Nota Bene : Le barème est donné à titre indicatif.

Exercice 1 – CRC (3 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 B6 (en hexadécimal).

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

Exercice 2 – Sous-Réseaux (3 pt)

On considère un réseau de classe B.

1. Combien de bits sont nécessaires pour définir 20 sous-réseaux ?
2. Combien de machines peut-on placer dans chaque sous-réseau ?
3. Quel est la valeur du masque de sous-réseau ?

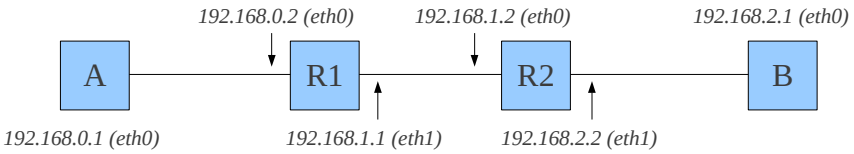
Exercice 3 – ATM (4 pt)

On considère le lien ATM à fibre optique s'étendant sur 400 km. La vitesse de propagation dans la fibre optique est de $2.5\ 10^5$ km/s. Le débit d'ATM est de 155 Mb/s. Contrairement à Ethernet qui utilise des trames de taille variable, ATM utilise des trames, appelées cellules, de taille fixe égale à 53 octets.

1. Calculer le temps de transmission t_{trans} d'une cellule.
2. Calculer la durée d'un trajet aller-retour t_{ar} (pour la distance maximale de 400 km).
3. Calculer le nombre minimum de cellules k pour que l'émetteur puisse envoyer des cellules de façon continue avant de recevoir le premier acquittement ($k.t_{trans} = t_{ar}$).
4. Quel est l'intérêt selon vous d'envoyer toujours un nombre minimum de k cellules ? Comment faire si le message de l'utilisateur ne contient que 10 octets ?

Exercice 4 (Routage et Firewall, 10 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 toutes les commandes nécessaires pour effectuer ce routage.
3. Supposons que A effectue un ping vers une adresse invalide, par exemple 192.168.3.1. On reçoit le message d'erreur ICMP « time-to-live exceeded » ! Expliquez ce qui se passe. Proposez une correction à cette situation.

Un firewall est installé sur la machine R2, avec DROP comme politique par défaut en INPUT, OUTPUT et FORWARD.

4. On suppose maintenant que la machine B héberge un serveur SSH (protocole TCP, port 22). Donnez la commande « iptables » sur R2, permettant à la machine A d'utiliser ce service SSH.
5. Un serveur Web (protocole TCP, port 80) est installée sur la machine R2. Donnez la commande « iptables » sur R2, permettant à la machine A d'utiliser ce service Web.

Memento Routage

- Activer le routage sur une machine (ip forward) : echo 1 > /proc/sys/net/ipv4/ip_forward
- Afficher la table de routage : route -n
- Définir une route par défaut : route add default gw <@gateway>
- Ajouter une route vers un réseau : route add -net <@network> netmask <mask> gw <@gateway>
- Ajouter une route vers une machine particulière : route add -host <@host> gw <@gateway>
- Pour supprimer une règle, il taper la commande route del <…> avec exactement les mêmes arguments que pour la commande add.

Memento Firewall

Voici quelques notes concernant l'utilisation d'iptables pour configurer un firewall. La configuration du firewall se base sur la table "filter" et est subdivisée en 3 chaînes (notée <CHAIN>) : INPUT : tout ce qui rentre dans la machine ; OUTPUT : tout ce qui sort dans la machine ; FORWARD : tout ce qui traverse la machine (i.e. lors du routage).

- Pour afficher les règles de la table filter : iptables -t filter -L
- Pour effacer toutes les règles ajoutées : iptables -t filter -F
- Pour chaque règle que l'on ajoute, trois actions sont possibles (notée <ACTION>) :
  - ACCEPT : on accepte ;
  - REJECT : on rejette poliment (réponse d'erreur envoyé à l'émetteur) ;
  - DROP : on jette à la poubelle (pas de réponse d'erreur).
- Pour modifier la politique par défaut du firewall : iptables -t filter -P <CHAIN> <ACTION>
- Pour ajouter une nouvelle règle à une chaîne du firewall (attention à l'ordre des règles) : iptables -t filter -A <CHAIN> <SRC> <DST> <...> -j <ACTION>
  - avec <SRC> des indications sur la provenance des paquets IP, comme par exemple "-i eth0" ou "-s 192.168.0.0/24" ou encore "-s 0/0" ;
  - avec <DST> des indications sur la destination des paquets IP, comme par exemple : "-o eth1" ou "-d 147.210.0.0/24" ;
  - avec <…> des infos complémentaires sur par exemple la nature du protocole "-p icmp" ou "-p tcp", avec éventuellement des precisions spécifiques à ces protocoles ("-dport 80" pour TCP) ou encore sur l'état "-m state -state NEW", …

Correction

Exercice 1 – CRC (3 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 B6 (en hexadécimal).

$(B6)_{16} = (1011\ \ 0110)_2$

$G(x) = x^3 + x + 1$
$M(x) = x^7 + x^5 + x^4 + x^2 + x$
$M(x).\ x^3 = x^{10} + x^8 + x^7 + x^5 + x^4$
On pose la division tel que $M(x).\ x^3 = G(x).Q(x) + C(x)$
$Q(x) = x^7 + x^2 + x + 1$
$C(x) = 1$
Donc la clef qui s'écrit sur 3 bits est 001.

Exercice 2 – Sous-Réseaux (3 pt)

1. 5 bits sont un minimum suffisant.
2. On peut placer $2^{(16-5)} - 2 = 2^{11} - 2 = 2046$ machines par sous-réseaux (si on enlève l'adresse de sous-réseau et l'adresse de broadcast).
3. Le masque du réseau de classe B est 255.255.0.0 ; le masque du sous-réseau est alors 255.255.XXX.0 avec $XXX = (1111\ 1000)_{binaire} = 248$, c'est-à-dire 255.255.248.0

Exercice 3 – ATM (4 pt)

1. Avec un débit de 155 Mb/s, le temps de transmission d'une cellule de 53 octets est de : $t_{trans} = (53 \times 8) / (155 \times 10^6) = 2.73\ \mu s$
2. La durée du trajet aller-retour s'écrit : $t_{AR} = (2 \times 400) / (2.5 \times 10^5) = 3.2$ ms
3. L'accusé de réception parviendra à la source après une durée t_{AR} . Pendant ce temps, il faut que la source envoie des cellules de manière continue. En d'autres termes, la taille minimum de la fenêtre doit être : $k = t_{AR} / t_{trans} = 3.2 \text{ X } 10^{-3} / 2.73 \times 10^{-6} = 1172$ cellules.
4. Cf. cours CSMA/CD. Si le message ne fait que 10 o, on rajoute des octets de « bourrage ».

Exercice 4 (Routage et Firewall, 10 pt)

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. Supposons que A effectue un ping vers une adresse invalide, par exemple 192.168.3.1. On reçoit le message d'erreur ICMP « time-to-live exceeded » ! Expliquez ce qui se passe. Proposez une correction à cette situation.
   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

   Un firewall est installé sur la machine R2, avec DROP comme politique par défaut en INPUT, OUTPUT et FORWARD.

4. On suppose maintenant que la machine B héberge un serveur SSH (protocole TCP, port 22). Donnez la commande « iptables » sur R2, permettant à la machine A d'utiliser ce service SSH.
   R2$ iptables -A FORWARD -s 192.168.0.1 -d 192.168.2.1 -p tcp --dport 22 -j ACCEPT
   R2$ iptables -A FORWARD -s 192.168.2.1 -d 192.168.0.1 -p tcp --sport 22
   -m state -- state ESTABLISHED -j ACCEPT

5. Un serveur Web (protocole TCP, port 80) est installée sur la machine R2. Donnez la commande « iptables » sur R2, permettant à la machine A d'utiliser ce service Web.
   R2$ iptables -A INPUT -s 192.168.0.1 -p tcp --dport 80 -j ACCEPT
   R2$ iptables -A OUTPUT -d 192.168.0.1 -p tcp --sport 80 -m state -- state ESTABLISHED -j ACCEPT