université de BORDEAUX

Collège Sciences et technologies

Année Universitaire	2013-2014	***Période***	Session de Printemps
Code Etape	MIAGE L3	***Code UE***	J1IN6026
Nom de l'Epreuve	Utilisation des Réseaux (session 2)		
Date / Heure	19/06/2014 à 14h00	***Durée***	1h30
Documents	Non autorisés	***Calculatrice***	Non
Nombre de pages	3	***Enseignant***	A. Esnard

Nota Bene : Le barème est donné à titre indicatif.

Ex 1 – Scapy (3 pt)

On considère la définition de la fonction mystere() suivante, utilisant Python/Scapy :

```
def mystere(host, maxval):
   for val in range(maxval):
      snd = IP(dst=host,ttl=val)/ICMP()
      rcv = sr1(snd,verbose=0)
      print snd.ttl, rcv.src
```

L'appel `mystere("www.google.fr",15)` donne le résultat suivant :

```
0 193.50.110.254
1 193.50.110.254
2 194.199.0.166
3 193.51.188.38
4 193.51.189.166
5 193.51.189.169
6 193.51.189.125
7 193.51.189.6
8 193.51.189.9
9 193.51.182.197
10 72.14.238.234
11 64.233.175.115
12 74.125.230.84
13 74.125.230.84
14 74.125.230.84
```

1. Expliquez l'objet de la fonction `mystere()` ?
2. Pourquoi les adresses IP des trois dernières lignes sont indentiques ?

Ex 2 – cours (2 pt)

1. En quelques lignes, expliquer le principe du NAT. A quoi cela sert-il ?
2. Quelle est le principal avantage de IPV6 sur la version actuelle de IP (IPV4) ?

Ex 2 – CRC & Hamming (4 pt)

On souhaite transmettre le message binaire M = 0111110.

1. Un protocole de communication utilise la méthode CRC pour la détection d'erreurs avec le polynôme générateur : $x^3 + x$. Calculer la clé CRC pour le message M en prenant soin de détailler les calculs.
2. On considère le code de Hamming (11,7) étudié en cours. Quel est le code de Hamming correspondant au message M ? On détaillera le calcul.

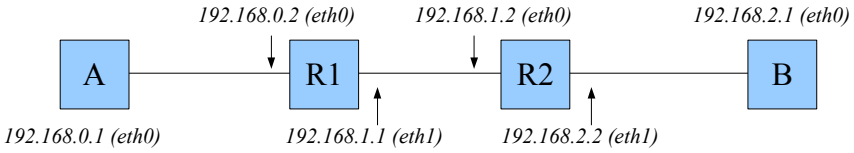
Ex 4 – Sous-Réseaux (3 pt)

On considère un réseau de classe B et on souhaite définir 20 sous-réseaux.

1. Combien de machines peut-on placer dans chaque sous-réseau ? Jusitifier.
2. Quel est la valeur du masque de sous-réseau ?

Ex 5 – Routage et Firewall (8 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.

Annexes

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 faut 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”, …