université de BORDEAUX

Collège Sciences et technologies

Année Universitaire	2015-2016	***Période***	Session de Printemps
Code Etape	MIAGE L3	***Code UE***	J1IN6026
Nom de l'Epreuve	Utilisation des Réseaux		
Date / Heure	03/05/2016 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 (Cours, 2 pt)

1. Expliquez brièvement les différentes couches du modèle standard TCP/IP, en citant des exemples de protocole à chaque niveau.
2. Expliquez brièvement le rôle du protocole ICMP. A quelle couche appartient ce protocole ?

Ex 2 (Code de Hamming, 4 pt)

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

1. Quel est le code de Hamming correspondant au mot 1110001 ?
2. Quel est le message correspondant au code 10001110101 ? Y a-t-il une erreur ? Si oui, corrigez-là (si possible).

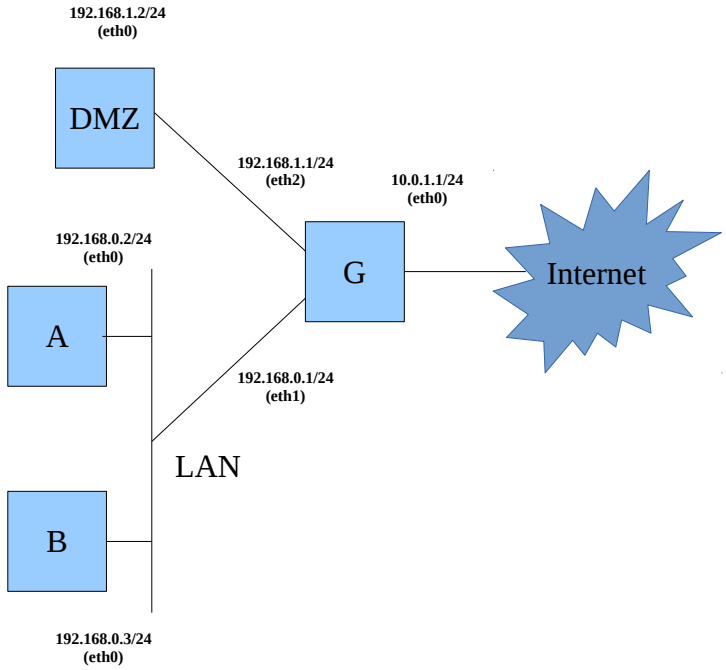
Ex 3 (Gigabit Ethernet, 4 pt)

Deux PCs sont reliés à un réseau par une liaison Gigabit Ethernet (débit à 1 Gb/s). Le support de transmission est un cable Ethernet classique sur lequel le signal électrique circule à 200 000 km/s. Ce réseau supporte des paquets IP de taille 576 octets.

1. Quel temps faut-il pour émettre un paquet IP ? On rappelle que la couche Ethernet rajoute 18 octets à la taille du paquet IP.
2. Les deux PCs sont à une distance raisonnable de 10m. Quelle est la durée de propagation du signal ?
3. Pourquoi le protocole CSMA/CD impose-t-il une taille minimale des trames Ethernet ?
4. Les cables Gigabit Ethernet classiques (norme 1000Base-T) supportent une longueur maximale de 100m. En déduire la taille minimale des trames Giga Ethernet.

Ex 4 (Administration, 10 pt)

On souhaite mettre en place un réseau domestique connecté à Internet par la passerelle G et organisé selon le schéma ci-dessous. La machine DMZ dispose d'un serveur SSH (port 22) et les machines du LAN utilisent régulièrement le web.



Pour chaque machine (sauf B), on demande de lister les commandes Linux nécessaires pour réaliser les tâches suivantes :

1. Configurer les IP.
2. Configurer le routage pour accéder à Internet.
3. Configurer le firewall sur la passerelle G conformément aux besoins énoncés.
4. Configurer le NAT dynamique sur la passerelle G. En quoi, est-ce utile ?
5. Configurer le port forwarding de G:2222 vers DMZ:22. En quoi, est-ce utile ?

Nota Bene : Vous disposez d'une annexe pour vous aider.

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", …

Memento NAT & Port Forwarding

- NAT Dynamique :G$ iptables -t nat -A POSTROUTING -o <iface> -j MASQUERADE (avec <iface> l'interface réseau permettant d'accéder à Internet)
- Port forwading :G$ iptables -t nat -A PREROUTING -i <iface> -p tcp --dport <P> -j DNAT --to <S>:<Q> (redirige le traffic de la connexion TCP/IP sur G:P vers S:Q avec G et S des adresses IP et P et Q des numéros de port)

Correction

Ex 1

cf. cours

Ex 2

1) Le code de Hamming de 1110001 est 11101101001

2) Dans le code 10001110101, P1 et P2 et P3 sont faux. L'erreur est donc en 7ème position (1+2+4=7) et on peut la corriger.

Ex 3

1) Temps émission = Taille / Débit = (576+18) octets / 1Gb/s = 594*8/10^9 = 4,752 µs

2) Durée propagation = Distance / Vitesse Propag. = 10 m / 200 000 km/s = 10 / 2*10^8 = 0.05 µs

3) Pour permettre la détection de collision de trame Ethetnet (cf. cours CSMA/CD).

4) Temps émission de la trame de poids min = Durée A/R à distance max

Donc, la taille min S_{min} = 2.(Distance / Vitesse Propag)*Débit = 2 . (100m / 2*10^8 m/s) * 1 Gb/s = 1000 bits = 125 octets. Dans la norme Ethernet (pas Gigabit), S_{min} vaut 64 octets.

Ex 4

```
1) IP

G$ ifconfig eth0 10.0.1.1/24
G$ ifconfig eth1 192.168.0.1/24
G$ ifconfig eth2 192.168.1.1/24
A$ ifconfig eth0 192.168.0.2/24
DMZ$ ifconfig eth0 192.168.0.2/24

2) Routage

A$ route add default gw 192.168.0.1
DMZ$ route add default gw 192.168.1.1
G$ echo 1 > /proc/sys/net/ipv4/ip_forward

3) Firewall

G$ iptables -P INPUT DROP
G$ iptables -P OUTPUT DROP
G$ iptables -P FORWARD DROP

Les machines du LAN accèdent au web :

G$ iptables -A FORWARD -s 192.0.0.0/24 -p tcp --dport 80 -j ACCEPT
G$ iptables -A FORWARD -d 192.0.0.0/24 -p tcp --sport 80 -m state --state ESTABLISHED -j
ACCEPT

La machine DMZ dispose d'un serveur SSH accessible :

G$ iptables -A FORWARD -d 192.0.1.2 -p tcp --dport 22 -j ACCEPT
G$ iptables -A FORWARD -s 192.0.1.2 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

4) NAT Dynamique, afin de permettre au machine du réseau privé d'accéder à Internet en
utilisant l'adresse publique de la passerelle G.

G$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

5) Port Forwarding, afin de rendre le service SSH (port 22) du réseau privé accessible sur
Internet via la passerelle G (port 2222).

G$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT --to 192.168.1.2:22
```