

<b>Année Universitaire</b>	2013-2014	<b>Période</b>	Session de Printemps
<b>Code Etape</b>	MIAGE L3	<b>Code UE</b>	J1IN6026
<b>Nom de l'Epreuve</b>	Utilisation des Réseaux		
<b>Date / Heure</b>	07/05/2014 à 11h00	<b>Durée</b>	1h30
<b>Documents</b>	Non autorisés	<b>Calculatrice</b>	Non
<b>Nombre de pages</b>	3	<b>Enseignant</b>	A. Esnard

Nota Bene : Le barème est donné à titre indicatif.

### Ex 1 (Cours, 3 pt)

1. Expliquez brièvement le principe d'acheminement d'un email en détaillant le rôle des serveurs et des protocoles utilisés. On pourra s'appuyer sur un schéma pour illustrer son propos.
2. Expliquez brièvement le rôle du protocole ARP dans un réseau local Ethernet.

### 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 1110011 ?
2. Quel est le message correspondant au code 10101110111 ? Y a-t-il une erreur ? Si oui, corrigez-là (si possible).

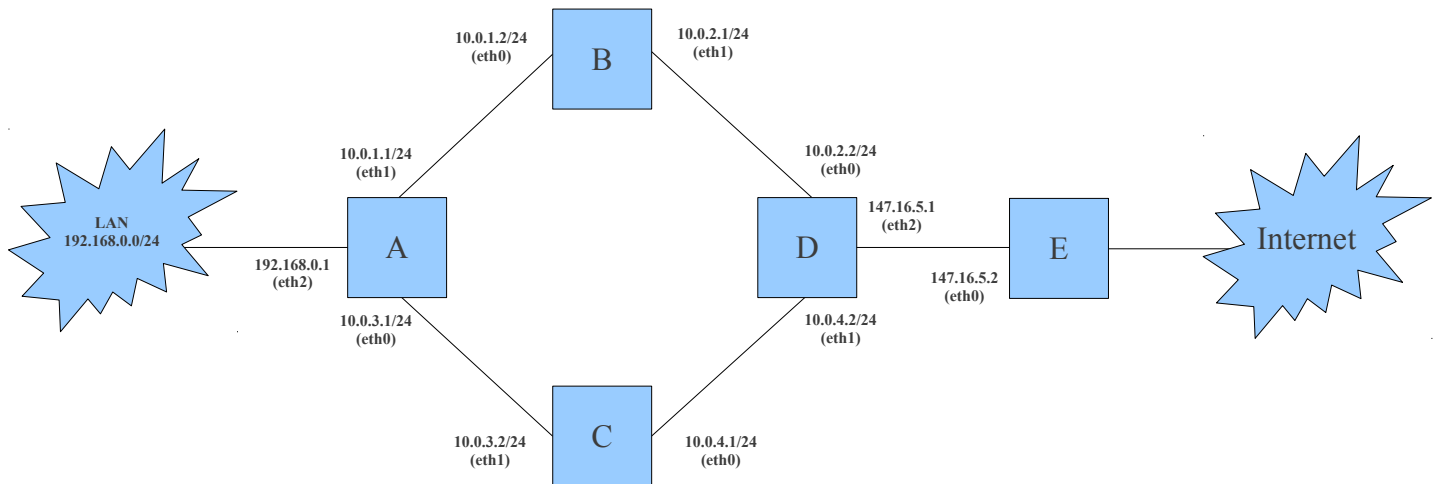
### Ex 3 (Sous-Réseaux, 3 pt)

On considère le réseau 80.10.0.0 / 16

1. Donnez le masque de ce réseau.
2. Combien de bits sont nécessaires pour définir 30 sous-réseaux ?
3. Combien de machines peut-on placer dans chaque sous-réseau ?
4. Quel est la valeur du masque de sous-réseau ?

## Ex 5 (Administration, 10 pt)

Nous considérons le réseau ci-dessous, connecté à Internet grâce aux routeurs A, B, C, D, et E. Vous administrez toutes les machines de ce réseau sauf E que l'on suppose correctement configuré. Soit X une machine du LAN et Y une machine sur Internet. Les parties A et B sont indépendantes.



**Partie A** – On souhaite faire en sorte que le trafic qui va du LAN vers Internet passe par le routeur B et celui qui va d'Internet au LAN passe par le routeur C.

1. Voici une configuration de routage proposée par un étudiant en MIAGE. Hélas, cette configuration est en partie fautive. Que se passe-t-il par exemple si une machine X du LAN envoie un ping à une machine Y sur Internet ?

```
X$ route add default gw 192.168.0.1
A$ route add default gw 10.0.1.2
B$ route add default gw 10.0.2.2
C$ route add default gw 10.0.3.1
D$ route add default gw 10.0.4.1
```

2. Proposez une solution pour corriger ce problème en donnant les commandes de routages nécessaires.

**Partie B** – On suppose que la configuration de notre réseau est maintenant réparée : toutes les machines peuvent se “parler” et se connecter à Internet. Nous allons mettre en place un firewall avec *iptables* sur la machine D.

3. Donnez les commandes pour configurer la politique par défaut à DROP.
4. Donnez les commandes pour autoriser les machines du LAN à “surfer” sur le Web (TCP/IP, port 80).
5. Soit Y, une machine sur Internet d'adresse 27.27.27.27. Modifiez le firewall sur la machine D, pour autoriser la machine Y à se connecter par SSH (TCP/IP, port 22) sur la machine A.
6. On s'intéresse maintenant à la configuration d'un firewall sur la machine Y. Comme dans la question précédente, on souhaite autoriser la connexion SSH de la machine Y sur la machine A. Donnez les commandes nécessaires.

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 précisions spécifiques à ces protocoles (`"-dport 80"` pour TCP) ou encore sur l'état `"-m state -state NEW"`, ...