Université de Montréal
Département d'informatique et de recherche opérationnelle
Session Hiver 2003
Professeur B. Jaumard

IFT3320 / IFT6320 – Téléinformatique
Devoir 2

A remettre le lundi 24 mars 2003 pour les questions 1 à 5,
et le lundi 31 mars pour la question 6.

Question #1 (IFT6320)

L'administrateur réseau d'une entreprise dispose de la technologie présentée à la figure 1 ci-dessous. Le routeur R2 est directement connecté à l'Internet et les routeurs R1, R3 et R4 sont reliés aux locaux de l'entreprise. R3 et R4 sont connectés à R2. Un garde-barrière situé entre R1 et R2 est sensé protéger l'entreprise des attaques de l'extérieur. Cependant, ses performances ne lui permettent pas de filtrer l'entièreté du trafic entrant et sortant. Pour contourner ce manque de performances, le nouveau gestionnaire du réseau propose de faire transiter le trafic entrant par le garde-barrière et le trafic sortant par les lignes R4-R2 et R3-R2.

1. Configurez les tables de routage des 4 routeurs pour répartir le trafic de cette façon.

2. Cette solution est-elle acceptable si le garde-barrière a pour objectif de n'autoriser que le trafic sur le port 80 vers des serveurs web du réseau de l'entreprise ? Discutez.

3. Cette solution est-elle acceptable si le garde-barrière a pour objectif d'autoriser uniquement le trafic qui a été initié par une machine se trouvant dans le réseau de l'entreprise ?

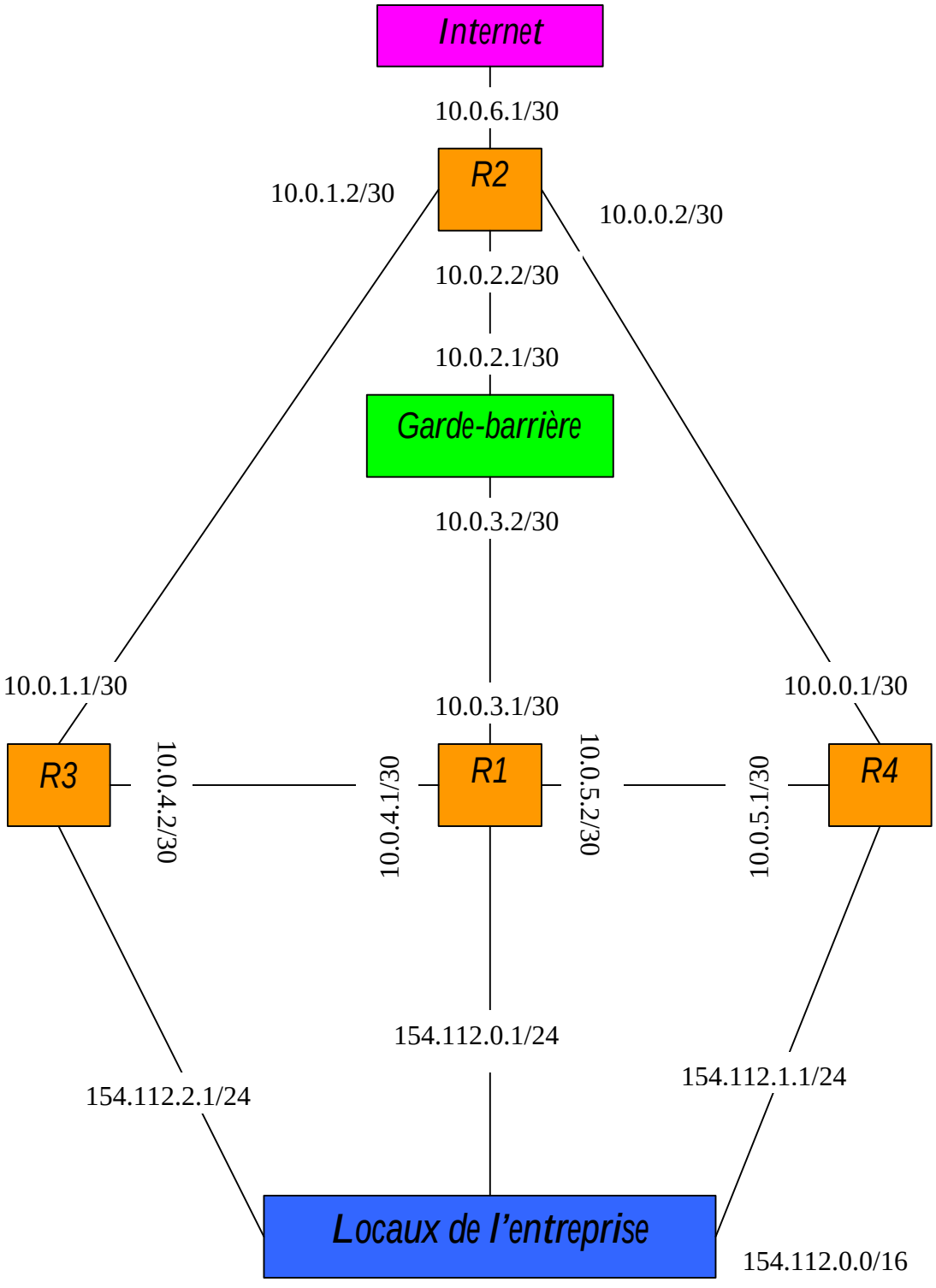


Figure 1. Organisation des routeurs d'accès de l'entreprise.

Question #2 (IFT3320/IFT6320) (voir la page web UncleFano, «*Pas d'utilisation prolongée sans avis médical.*» , perso.club-internet.fr/spinard/exo_ip3.htm)

Indiquez si les adresses suivantes sont valides ou pas pour un hôte TCP/IP. Si une adresse est invalide, entourez la partie erronée et fournissez une explication. Le masque est celui associé par défaut à la classe.

1. 245.12.33.102
2. 123.123.123.123
3. 199.23.107.255
4. 199.23.107.0
5. 156.266.12.103
6. 99.0.0.12
7. 153.0.0.0
8. 153.0.0.255
9. 191.23.255.255
10. 32.255.255.0
11. 12.0.0.0
12. 12.255.255.255

Question #3 (IFT3320/IFT6320) (voir perso.club-internet.fr/spinard/exo_ip9.htm)

Calculez le masque adapté aux exigences du scénario :

- indiquez le nombre exact de sous-réseaux créés par votre masque
- indiquez également le nombre exact d'hôtes par sous-réseau.

Scénario 1	
Nombre de segments physiques requis :	**5**
Nombre maximum d'hôtes par segment :	**25**
Adresse de réseau :	**192.177.4.0**
Masque de sous-réseau proposé :	**……**
Nombre de sous-réseaux créés :	**……**
Nombre maximum d'adresses par segment :	**……**

Scénario 2	
Nombre de segments physiques requis :	**100**
Nombre maximum d'hôtes par segment :	**88000**
Adresse de réseau :	**39.0.0.0**
Masque de sous-réseau proposé :	**……**
Nombre de sous-réseaux créés :	**……**
Nombre maximum d'adresses par segment :	**……**

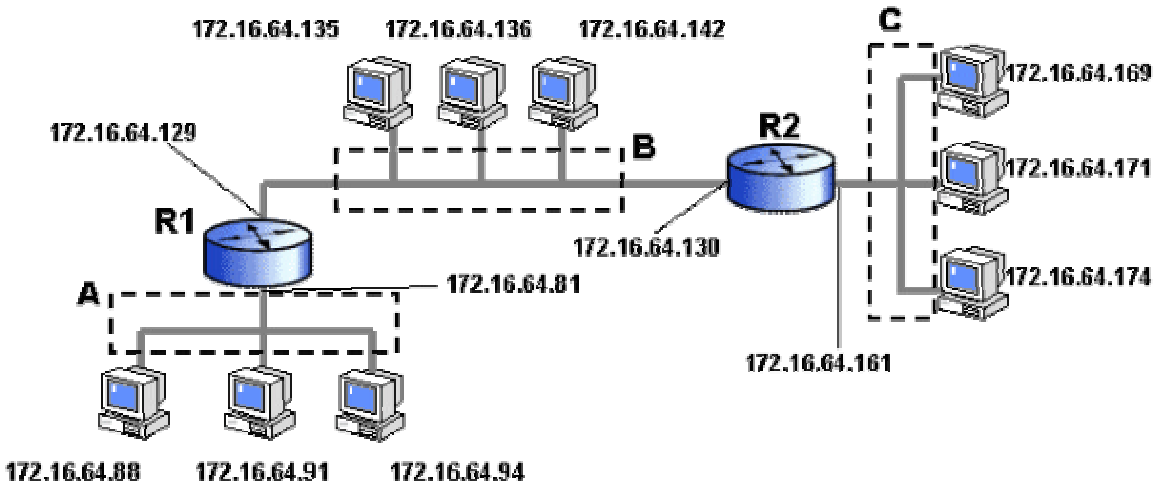
Scénario 3	
Nombre de segments physiques requis :	**100**
Nombre maximum d'hôtes par segment :	**350**
Adresse de réseau :	**117.133.0.0**
Masque de sous-réseau proposé :	**……**
Nombre de sous-réseaux créés :	**……**
Nombre maximum d'adresses par segment :	**……**

Scénario 4	
Nombre de segments physiques requis :	**12**
Nombre maximum d'hôtes par segment :	**12**
Adresse de réseau :	**216.121.44.0**
Masque de sous-réseau proposé :	**……**
Nombre de sous-réseaux créés :	**……**
Nombre maximum d'adresses par segment :	**……**

Scénario 5	
Nombre de segments physiques requis :	**50**
Nombre maximum d'hôtes par segment :	**600**
Adresse de réseau :	**134.119.0.0**
Masque de sous-réseau proposé :	**……**
Nombre de sous-réseaux créés :	**……**
Nombre maximum d'adresses par segment :	**……**

Question #4 (FT3320/IFT6320) (voir la page web UncleFano, «*Pas d'utilisation prolongée sans avis médical.*» , perso.club-internet.fr/spinard/exo_ip16.htm)

Configuration de routeurs. Vous concevez le réseau suivant avec l'objectif de maximiser le nombre de réseaux :



1. Quel masque avez-vous probablement utilisé ?
2. Afin d'économiser la bande passante et parce que ça n'aurait que peu d'intérêt, vous renoncez à mettre RIP en œuvre. Notez la syntaxe que vous utiliserez pour configurer les routeurs R1 et R2.

Question #5 (IFT3320/IFT6320) (Examen final, IFT3320/IFT6320, automne 2002, question 7)

Un commutateur ATM dispose de 16 lignes SONET STS-1 (51,84 Mbps) d'entrée et 16 lignes de sortie.

1. Quel est le débit utilisateur d'un lien SONET STS-1 ?
2. Quelle capacité globale en bit/s doit offrir le commutateur pour supporter la charge ?
3. Combien de cellules ATM le commutateur doit-il traiter par seconde ?

Question #6 IFT3320/IFT6320 Etude du système de chiffrement à clé publique RSA

On rappelle l'algorithme du MIT (Rivest, Shamir et Adleman, 1978).

- ✓ Choisir deux nombres p and q premiers et grands ($p, q > 10^{100}$).
- ✓ Calculer $n = p \times q$ et $z = (p-1) \times (q-1)$.
- ✓ Soit d un nombre premier avec z (z et d sont premiers entre eux).
- ✓ Déterminer un nombre e tel que $e \times d = 1 \bmod z$.

Soit A un message binaire. Découper A en blocs de k bits tel que k soit le plus grand entier tel que $2^k < n$.

Soit P un bloc de k bits, le codage de P est donné par : $C = E(P) = P^e \pmod n$.

Le déchiffrage d'un message crypté C est donné par : $P = D(C) = C^d \pmod n$

1. On donne les valeurs numériques suivantes : $p = 3$, $q = 11$ (trop petites en pratique, mais traitable en exercice).

   Calculer les valeurs des nombres d et c vérifiant les conditions de l'algorithme du MIT. Pour avoir un couple unique on prend la plus petite valeur possible de d et pour cette valeur la plus petite valeur possible de e.

   Quelle est la clé publique et quelle est la clé secrète ?

2. Soit le message de 3 chiffres 1, 6, 15 soit par blocs de 5 bits la configuration de bits suivante :

   00001 00110 01111.

   Coder ce message en utilisant les paramètres de chiffrement RSA précédents.

3. Soit le message suivant par blocs de 6 bits (4, 14, 24) :

   000100 001110 011000

   Donner la valeur initiale du message (texte en clair), en prenant les mêmes valeurs pour d, e et k qu'à la question 2.

4. Pourquoi ne peut-on pas prendre p et q petits ?

   Que se passe t-il lorsque p et q sont de l'ordre de 10^{10} ?