Université Paris Diderot
M2 informatique
Protocoles et services internet
2012

Examen Protocoles et Services Internet

(durée 2 heures, documents interdits)

Tous les exercices sont indépendants.

Exercice 1.— (maximum 3 lignes par question) On considère le fichier html correspondant à l'url `http:www.x.fr:/exam.html` (on suppose que le serveur http correspondant à `www.x.fr` est correctement configuré):

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
  <head>
    <meta content="text/html; charset=ISO-8859-1"
      http-equiv="Content-Type">
    <meta content="sans" name="author">
    <title>exam</title>
  </head>
  <body>
    Bonjour<br>
    Une <a href="images/gradient.jpg"> un lien sur image</a> et un <a
      href="http://www.univ-paris-diderot.fr/index.html">lien</a> et une
    <a href="#bal"> ancre</a><br>
    et <img alt="image1"
        src="http://www.liafa.jussieu.fr/~hf/images/image013.jpg"
        height="47" width="47">,<br>
    aussi<img alt="image2" src="IMG_0150.jpg" height="101" width="89"> <br>
    <a name="bal"></a>une ancre.<br>
  </body>
</html>
```

1. Donner la liste des *objets* contenus dans cette page en précisant leur type (image, lien vers une url, ...).
2. Décrire rapidement en précisant en particulier ce qu'il advient en ce qui concerne les objets de la page ce que provoquent les lignes de codes suivantes (on suppose que ces lignes sont suivies de deux retours à la ligne)

   (a)
   ```
   telnet www.x.fr 80
   GET /exam.html HTTP/1.1
   Host: www.x.fr
   Connection: close
   ```

   (b)
   ```
   telnet www.x.fr 80
   GET /exam.html HTTP/1.1
   Host: www.x.fr
   ```

   (c) Pour obtenir le contenu complet de la page, combien de connexions avec le serveur `www.x.fr` sont nécessaires dans un mode persistant et dans un mode non-persistant? Combien de connexions au total sont nécessaires dans chacun de ces deux modes?

Exercice 2.— (maximum 3 lignes par question) Soit u une page web sur le serveur s, u contient uniquement des références à des fichiers $f_1, \cdots, f_m$ qui sont tous sur le même serveur. On suppose que le temps pour obtenir f_i (requête http + temps de la réponse) est rtt_i et que le temps pour établir une connexion vers le serveur est t_s.

1. Quel est le temps total pour obtenir la page complète en mode persistant? En mode non-persistant? En mode non-persistant avec un navigateur configuré pour k connexions en parallèle?
2. On suppose que l'adresse IP du serveur n'est pas dans le cache de l'hôte local. En quoi consiste le temps de la connexion? Le temps de la deuxième connexion vers le serveur sera-t-il identique au temps de la première?

Exercice 3.— (maximum 3 lignes par question)

1. A quoi sert un DNS?
2. A quoi correspondent les serveurs DNS racines? les "top-level domain" (TLD) serveurs? les "authoritative" DNS serveurs?
3. Quelle est la différence entre le mode récursif et itératif?
4. Comment le DNS peut servir à répartir la charge?
5. Pourquoi un DNS est un élément important concernant la sécurité?

Exercice 4.— (maximum 4 lignes par question)

1. On dispose d'un système à clé symétrique partagée (uniquement) par Alice et Bob. On suppose que Alice veut transmettre le message m à Bob. Décrire une façon très simple pour Alice de transmettre m à Bob permettant de garantir à Bob que le message reçu provient bien de Alice? Quel est l'inconvénient majeur de cette façon de faire? Ce procédé garantit-il la propriété de non-répudiation?
2. On suppose maintenant que Alice a une clé privée et que sa clé publique est connue de Bob. On suppose que Alice veut transmettre le message m à Bob. Décrire une façon simple pour Alice de transmettre m à Bob permettant de garantir à Bob que le message provient bien de Alice? Ce procédé garantit-il la non-répudiation ? Comment garantir toujours la propriété de non répudiation?
3. Pourquoi de nombreux protocoles utilisent des systèmes à clés symétriques et limitent l'usage de systèmes à clés publiques?

Exercice 5.— On considère un système de l sites dans lequel chaque site a comme identité un mot $b_{n-1} \cdots b_0$ où chaque b_i est 0 ou 1 qu'on interprètera comme un entier entre 0 et $2^n - 1$ (on suppose que le nombre de site est 2^n). Chaque site d'identité k maintient une table V_k qui contient les adresses IP des sites auxquels il est connecté (un élément de V_k est un couple $(m, ip(m))$ où m est l'identité d'un site et $ip(m)$ l'adresse IP de ce site).

1. Pour tout site k, V_k contient uniquement le couple $((k+1) \bmod 2^n, ip((k+1) \bmod 2^n))$. Décrire un protocole simple qui permet pour un site source d'envoyer un message à n'importe quel site à partir des identités. Dans le cas le pire, combien de sites peut-on être amené à traverser pour envoyer un message?
2. Pour tout site k, V_k contient les couples $((k+2^i) \bmod 2^n, ip((k+2^i) \bmod 2^n))$ pour i compris entre 0 et $n-1$.

   Décrire un protocole qui permet pour un site source quelconque d'envoyer un message à n'importe quel site destinataire à partir des identités. Dans le cas le pire, combien de sites peut-on être amené à traverser pour envoyer un message? Quelle est en fonction de l, la taille des tables V_k et, dans le pire cas, le nombre de sites à traverser pour envoyer un message?