Université Paris Diderot
M2 informatique
Protocoles et services internet
2016-2017

Examen Protocoles et Services Internet

(durée 2 heures documents autres que manuscripts interdits)

2 pages

Tous les exercices sont indépendants. La plupart des questions sont des questions de réflexion pour lesquelles plusieurs réponses peuvent être admises si elles sont correctement justifiées. **Vous répondrez en au plus 5 lignes à chaque question.**

Exercice 1.—

1. Qu'est ce que le DNS, quel est son rôle? Décrire dans les grandes lignes son fonctionnement.
2. Lorsqu'un client interroge sur DNS sur un site X, est ce que le DNS fournit au client une route vers X?
3. Comment le DNS peut servir à répartir la charge?
4. Pourquoi un DNS est un élément important concernant la sécurité?
5. Comment expliquez vous que lorsque avec votre ordinateur portable et une connexion en France, la page de google vous donne Google France. Et si vous êtes dans un autre pays vous accédez au Google local?

Exercice 2.— 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.—

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? Ce procédé garantit-il la propriété de confidentialité du message? 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 propriété de confidentialité du message? Ce procédé garantit-il la propriété de non-répudiation?
3. On suppose en plus que Bob a une clé privée et que sa clé publique est connue d'Alice. Comment garantir les propriété de non répudiation et confidentialité du message?

4. Pourquoi de nombreux protocoles utilisent des systèmes à clés symétriques et limitent l'usage de systèmes à clés publiques?

Exercice 4.— Expliquer succinctement en quoi consiste le modèle client serveur. Même question pour le modèle pair à pair. Au niveau des connexions avec des sockets (par exemple Java), la notion de pair à pair a-t-elle du sens? Si non pourquoi et si oui de quelle façon?

Pour trouver les données dans un système pair à pair, on peut utiliser des filtres de Bloom ou des DHT (Distributed Hash Table). Comment fonctionnent ces mécanismes?

Exercice 5.—

1. Soit A un ordinateur portable qui peut donc se connecter sur différents réseaux locaux. En supposant que A soit identifié par une adresse IP sur un réseau fixe particulier, proposer une (des?) solutions pour assurer qu'il soit joignable sur le réseau local sur lequel il est à un moment donné.
2. Si maintenant A est identifié par un nom internet, comment peut-on procéder?