Université Paris Diderot
M2 IAP et MIC
Protocoles des services internet
2018-2019

Examen
Protocoles des Services Internet

(durée 2 heures, documents interdits)

Les 3 exercices sont indépendants. Le barème est donné à titre indicatif.

Exercice 1.— (7 points)

1. Quel est le rôle du DNS?
2. Le DNS est-il organisé de manière hiérarchisée? Si oui décrivez cette hiérarchie.
3. Le DNS est-il utilisé pour le courrier ? Si oui indiquez comment.
4. Le site web d'une compagnie est assuré par différents serveurs. Comment le DNS peut-il servir à répartir la charge entre ces serveurs?
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?
6. Lorsqu'un client interroge le DNS sur un site X, est-ce que le DNS fournit au client une route vers X?
7. Paul a réalisé une application web sur un ordinateur qui se trouve sur le réseau avec une adresse IP et il voudrait que les internautes puissent y accéder par un nom. Est-ce possible? Si oui, que doit-il faire?

Exercice 2.— (6 points) Bob et Alice sont deux collègues. Ils se rencontrent et se mettent d'accord sur la manière dont ils vont communiquer pour que lorsqu'Alice reçoit en message de Bob, elle soit sûre que le message a bien été écrit par Bob et que personne d'autres n'a pu lire le contenu.

1. Proposez à Alice et Bob un protocole pour leurs échanges et indiquez les éléments sur lesquelles ils doivent se mettre d'accord lors de leur rencontre. Dans ce protocole, indiquez comment est assuré:
   (a) la confidentialité
   (b) l'authentification de l'expediteur
2. Bob publie des informations sur un site Web et Alice voudrait pouvoir vérifier que c'est bien Bob qui les a publiés. Proposez à Alice et Bob un protocole et indiquez les éléments sur lesquelles ils doivent se mettre d'accord lors de leur rencontre.
3. Trudy n'aime pas Alice et Bob. Est ce qu'elle peut leur nuire dans les protocoles que vous avez proposés? Si oui, comment?

Exercice 3.— (7 points) On veut réaliser une DHT. On considère un système d'au plus 2^n 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 $2^n - 1$. 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 et un port).

On a aussi des fichiers qui sont identifiés par un mot $b_{n-1} \cdots b_0$ où chaque b_i est 0 ou 1.

Le site k_s est le premier site d'identité supérieure à k dans le système (modulo 2^n) et le site k_p est le premier site d'identité inférieure à k dans le système(modulo 2^n).

Le site k sait où trouver le contenu du fichier ou si le fichier n'existe pas pour tous les fichiers identifiés par un entier entre k et $k_s - 1$.

On propose 2 architectures:

1. Pour tout site k, V_k contient les couples $(i, ip(i))$ pour tous les sites i.
2. Pour tout site k, V_k contient les couples $(k_s, ip(k_s))$ et $(k_p, ip(k_p))$.

1. Pour les 2 architectures : décrire un protocole qui permet pour un site de pouvoir obtenir des informations sur un fichier dont il connait l'identifiant (accès au contenu ou non existence du fichier sur la DHT). Dans le pire cas, combien de sites peut-on être amené à traverser pour envoyer un message?

   Décrivez les opérations à faire en cas de départ ou d'arrivée d'un site (on suppose qu'un seul site se déconnecte, le reste de la DHT étant stable. De même on suppose qu'un seul site demande à appartenir à la DHT le reste étant stable et que ce site connait un des sites composant la DHT.)

2. Proposez ce qui vous semble le "meilleur" choix d'architecture de DHT (une des 2 précédentes ou une autre), indiquez comment vous l'implémenteriez, précisez si vous choisiriez des connexions TCP ou UDP. Indiquez la taille de la table de chaque site, le cout de l'ajout et de la suppression d'un site, le cout de la recherche d'un fichier par un site et pourquoi vous avez fait ce choix.