INF8480

Module 1 : Réseau

1.1 Un client envoie une requête de 200 octets et reçoit une réponse de 5000 octets. Quel est le temps total requis avec les hypothèses suivantes, pour UDP, TCP, local: latence de réseau 5ms, ouvrir une connexion TCP 5ms, débit 10Mbits/s, unité de transfert maximale 1000 octets, temps de traitement 2ms, réseau peu chargé? En local, la latence est de 2ms et le débit mémoire-mémoire de 400Mo/s.

Un client envoie une requête de 200 octets et reçoit une réponse de 5000 octets.

UDP (datagram): 5ms + (200 * 8) / 10000bits/ms + 2ms + 5 (5 + (1000 * 8) / 10000bits/ms) = 36.16ms

TCP (avec connexion): 5ms + 5ms + (200 * 8) / 10000bits/ms + 2ms + 5 (5 + (1000 * 8) / 10000bits/ms) = 41.16ms (suivi d'accusé de réception).

Accès local: en supposant une latence de 2ms en local dans les deux directions et un transfert mémoire mémoire de 400 mégaoctets/s, 2ms + 200 / 400000 octets/ms + 2ms + 5000 / 400000 octets/ms = 4.013ms.

1.2 Quel est la tâche d'un routeur sur l'Internet? Quelles tables doit-il maintenir?

Un routeur connecte plusieurs réseaux IP. Il reçoit des paquets de ces réseaux et pour chacun doit décider à quel réseau l'envoyer. Il doit avoir une table qui dit, pour chaque groupe d'adresse IP possible, vers quel réseau l'envoyer pour que le paquet atteigne sa destination par le meilleur chemin possible. Etant donné le très grand nombre de réseaux sur l'Internet, on ne peut avoir une table complète à chaque routeur. A la place, des routes par défaut et des regroupements de réseaux existent et servent à minimiser les tables (e.g. route par défaut vers un routeur avec une table plus complète, groupe de réseaux qui commence par XXXX envoyé vers un routeur en Asie où se trouvent tous ces réseaux).

1.3 Comment sait-on que toutes les adresses IP sont uniques?

Un centre s'occupe d'allouer les adresses IP et ne donne jamais la même adresse 2 fois. Si quelqu'un choisit une adresse au hasard sans passer par ce centre, cela peut causer des ennuis sérieux.

1.4 Quel est le meilleur choix, TCP ou UDP, pour chacune des applications suivantes: Telnet, FTP, HTTP, RPC?

Telnet: la fiabilité est importante et la performance n'est pas un problème, TCP est plus simple à utiliser.

FTP: pour le transfert de très gros fichiers, les possibilités de fenêtres d'accusés de réception, retransmission, contrôle du débit... de TCP sont très utiles.

HTTP: pour de courtes réponses, UDP pourrait être intéressant. Cependant, les transferts impliquent assez souvent de gros fichiers ou des requêtes multiples sur la même connexion et TCP est donc utilisé.

RPC: les messages sont généralement courts et un système de délai expiré est déjà implanté. UDP est donc un choix efficace dans ce contexte.

1.5 Avec telnet, les messages spéciaux comme KILL doivent être prioritaires (e.g. pour arrêter le défilement d'un gros fichier). Comment cela est-il implanté?

Lorsque les tampons du récepteur sont pleins, le message KILL ne serait normalement pas accepté. Heureusement, le paquet peut avoir l'attribut urgent auquel cas il court-circuite la queue de réception de la connexion TCP.

1.6 Un serveur ouvre un port et lui assigne un nom (numéro). Comment les clients peuvent-ils s'y connecter?

L'adresse d'un service est constituée de l'adresse IP et du numéro de port. On peut utiliser une adresse pré-établie (e.g. 132.207.99.1 pour la passerelle du réseau 132.207.99), un nom qui doit être communiqué (e.g. charles.polymtl.ca), ou un nom par convention (e.g. www.polymtl.ca, news.polymtl.ca).

Pour les numéros de ports, les numéros pré-établis sont souvent utilisés (e.g. 21 FTP, 22 SSH, 23 TELNET). Le service portmap existe aussi mais est principalement utilisé pour les Sun RPC.

1.7 Discutez des principaux types de problèmes de sécurité sur l'Internet.

Le premier type d'attaque est d'utiliser un processus sur le serveur pour y prendre pied. Ce processus peut être mal configuré (contrôle des accès), mal protégé (mot de passe par défaut), ou mal programmé (débordement de tampon). Un deuxième type d'attaque est de corrompre le réseau en espionnant ce qui s'y passe ou en falsifiant la provenance de messages. Un troisième type d'attaque est le déni de service en surchargeant un serveur ou un réseau de manière à le rendre inopérant.

1.8 Une passerelle pare-feu peut-elle protéger contre une attaque par déni de service?

Difficilement car les paquets en volume trop élevé peuvent être corrects et satisfaire les règles vérifiées par le coupe-feu. Même si ces paquets sont invalides selon les règles du coupe-feu, celui-ci sera surchargé et ne pourra s'occuper adéquatement des paquets corrects.