Année Universitaire 2010-2011 session 1 d'automne

Parcours : CSB5 Licence 3 STS Informatique **UE :** INF157
Épreuve : Examen Utilisation des réseaux
Date : 13 décembre 2010 **Heure :** 8h30 **Durée :** 1h30
Modalités : Épreuve sans document, avec calculatrice
Épreuve de : Mr Samuel Thibault 3 pages

Exercice 1. Questions de cours (5 pt)

Q1.1 Faites un schéma pour représenter l'empilement habituel des protocoles Ethernet, IP, TCP et UDP.

Q1.2 Donnez la première ligne d'une requête HTTP (version 1.1) demandant le document `bobi.txt` situé dans le répertoire `tmp` du serveur web `foo.com` interrogé. Donnez la première ligne de la réponse HTTP de celui-ci, lorsqu'il n'a pas trouvé le document demandé. (2 lignes max)

Q1.3 Pourquoi préfère-t-on pour le protocole ssh utiliser TCP plutôt que UDP, alors que pour DNS on se permet d'utiliser UDP ?

Q1.4 À quoi sert une passerelle ?

Q1.5 Un correspondant au Japon m'a envoyé par mail une archive .zip contenant un document sur lequel il vient de travailler. Mon dézippeur affirme que le document vient du futur ! Que s'est-il passé, qu'aurait-il dû se passer ? (Il m'affirme que son ordinateur est bien à l'heure)

Q1.6 Quels sont tous les protocoles et machines potentiellement mises en œuvre lorsque l'on lance la commande `ping -c 1 www.tfou.fr` ? Énumérez les paquets émis et reçus par la carte réseau de la machine où l'on lance la commande (on supposera que la machine vient juste d'être allumée).

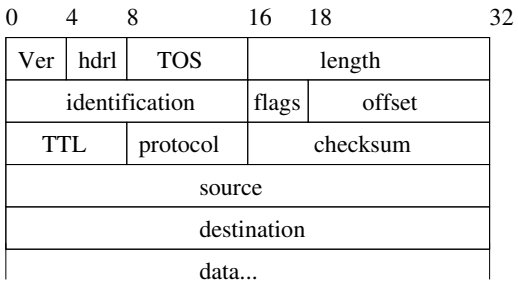
Q1.7 En quoi la version *threads* d'un serveur echo est-elle plus simple qu'une version `select` ?

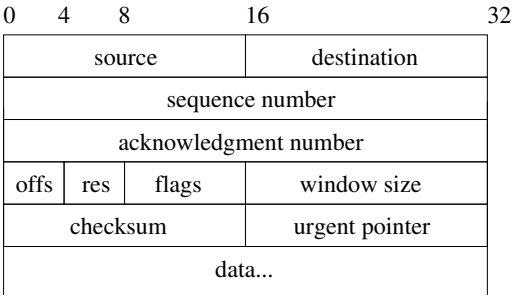
Exercice 2. Analyse de paquet

Voici un paquet IP capturé par *wireshark*, contenant un extrait de connexion ssh (dont on rappelle que le numéro de port est 22) :

```
0x00:  45 00 00 48 5d cb 40 00 3a 06 16 2f 0b 0c 0d 0e
0x10:  0b 0c 0d 0f 00 16 04 01 f7 90 50 b5 18 fa 80 3f
0x20:  80 18 00 2e 47 f2 00 00 01 01 08 0a 1c 92 0d 8a
0x30:  00 3a b7 ac 53 53 48 2d 32 2e 30 2d 4f 70 65 6e
0x40:  53 53 48 5f 34 2e 33 0a
```

On rappelle le format des en-têtes IP et TCP :





Quelle est l'adresse IP du serveur sshd, et l'adresse IP du client ssh ? Quel est le numéro de port utilisé du côté du client ?

Exercice 3. Calculs de débits

Deux fous utilisent des clés USB de 32Go et des lance-pierres pour s'échanger des données. Le temps de vol d'une clé USB entre les deux fous est d'environ une seconde. Le temps de préparation du lance-pierre (pose, visée, tir) est d'environ deux secondes, et le temps de réception est d'environ une seconde.

Q3.1 Dans un premier temps, on considère qu'ils ont tous deux des clés USB contenant déjà les données prêtes à envoyer, et qu'ils n'ont pas besoin de lire celles qu'ils reçoivent immédiatement. Quels sont le débit et la latence de ce moyen de communication ? (expliquez votre calcul)

Q3.2 Maintenant, un des deux fous veut envoyer à l'autre un gros fichier de son ordinateur portable, en le découpant en morceaux de 32Go. La vitesse de transfert entre l'ordinateur et la clé USB est de 10Mo/s. On négligera le temps de débranchement/rebranchement de clé USB. Quels sont le débit et la latence du transfert vers l'ordinateur de l'autre fou ? (expliquez votre calcul)

Q3.3 Le fou émetteur vise en fait assez mal, et un certain nombre de clés USB sont ainsi perdues en chemin (heureusement, ils en ont en réserve). En vous inspirant d'un protocole bien connu, expliquez brièvement comment les deux fous peuvent s'assurer que le fou récepteur reçoit correctement le fichier.

Exercice 4. Voici la configuration d'une machine :

```
$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:21:70:b4:36:49
          inet adr:169.254.255.8  Bcast:169.254.255.255  Masque:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:273345 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:86514668 (82.5 MiB)  TX bytes:23180492 (22.1 MiB)
$ /sbin/route
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         169.254.0.1     0.0.0.0         UG    0      0        0 eth0
$ /usr/sbin/arp
Address                  HWtype  HWaddress           Flags Mask            Iface
```

Q4.1 Quelle sont l'adresse MAC et l'adresse IP de la machine ?

Q4.2 Quel est l'ensemble des adresses IP accessibles directement ?

Exercice 5. On désire implémenter un jeu d'échecs en ligne permettant d'obtenir une liste d'adversaires potentiels, en choisir un et jouer contre lui. On réfléchit au protocole que l'on va inventer pour cela.

Q5.1 On a vu en cours qu'un protocole peut être centralisé, décentralisé, ou bien acentré. Qu'est-ce que cela voudrait dire en pratique dans ce contexte de jeu d'échec en ligne ?

Q5.2 On se propose d'écrire un client que les utilisateurs lanceront sur leur machine. Quelles informations fera-t-on passer sur le réseau ?

Q5.3 Le service marketting nous indique qu'il faudrait que le jeu puisse fonctionner depuis un simple navigateur web mais en conservant un rendu 3D de l'échiquier. En supposant que les navigateurs webs

disposent de l'extension javascript ou flash, quelles sont toutes les informations que l'on fera passer sur le réseau ?

Q5.4 Le service clientèle indique que des utilisateurs se sont plaints de ne pas pouvoir jouer sans extension javascript ni flash. Quelle version simplifiée peut-on fournir ?

Exercice 6. PGP

Le système cryptographique PGP est basé sur des paires de clés publique/privée. Toute personne désirant utiliser PGP génère une paire de clés publique/privée, garde la partie privée secrète, et publie la partie publique le plus largement possible en la mettant à disposition sur des serveurs publics bien connus, sur lesquels n'importe qui peut déposer des clés publiques à volonté, et où n'importe qui peut les récupérer.

Q6.1 Alice a généré une paire de clés et Bob en a récupéré la partie publique. Ils peuvent alors utiliser les clés dont ils disposent ainsi pour protéger plus ou moins les messages qu'ils échangent. Qui peut envoyer des message cryptés à qui ? Qui peut envoyer des messages signés à qui ?

Q6.2 Il n'est pas très fiable de déposer simplement une clé publique sur un serveur public ; que pourrait faire quelqu'un mal intentionné ?

Le plus sûr est de se rencontrer physiquement pour pouvoir s'échanger en main propre des clés publiques, mais ce n'est pas toujours possible. C'est pour cela qu'en fait, un utilisateur dépose sur les serveurs publics une version de sa clé publique *signée* par d'autres personnes, dont il suffit ainsi d'avoir la clé publique pour pouvoir être sûr que la clé signée est bien digne de confiance.

Q6.3 Bob génère aussi une paire de clés. Ni Bob ni Alice n'ont le temps de se déplacer pour s'échanger leurs clés publiques en mains propres. Cependant, un ami commun Joe, aussi utilisateur de PGP, va bientôt déménager : il pourra rencontrer physiquement Alice puis Bob (mais ne reviendra pas voir Alice). Expliquez comment procéder pour que Bob et Alice puissent échanger leurs clés publiques de manière sûre.