Année Universitaire 2017-2018 session 1 d'automne

**Parcours :** TAH Licence pro ADSILLH **UE :** 4TAH501U
**Épreuve :** Examen réseaux
**Date :** 24 novembre **Heure :** 14h30 **Durée :** 1h30
**Modalités :** Épreuve sans document, calculatrice autorisée
**Épreuve de :** Mr Samuel Thibault 2 **pages**

université de BORDEAUX

Collège Sciences et technologie

**Exercice 1.** Questions de cours

**Q1.1** Quelle est la différence entre HTTP et HTML ?

**Q1.2** Un collègue met en place un petit site web avec une authentification par mot de passe. Que doit-il penser à activer pour éviter un problème de sécurité, pourquoi ?

**Q1.3** Pourquoi IP et TCP sont deux protocoles séparés ?

**Q1.4** Deux groupes d'étudiants écrivent chacun un jeu de pong en réseau. Ils décident d'utiliser le même protocole, avec un encodage binaire des données plutôt qu'un encodage textuel. Les coordonnées x et y des balles (typiquement entre 0 et 300) sont ainsi chacune échangée sous forme d'entier 16 bits codé en binaire dans le flux TCP. Chaque groupe travaille d'abord sur son implémentation dans son coin, et obtient une version fonctionnelle. Ils décident alors de connecter les deux implémentations, et c'est là que les ennuis commencent... Les coordonnées échangées sont très bizarres : une implémentation envoie par exemple les coordonnées (100,100), mais l'autre implémentation reçoit les coordonnées (25600,25600).

Que s'est-il passé ? Qu'aurait-il dû se passer ?

**Q1.5** Expliquer la différence entre "acentré", "centralisé", "décentralisé".

**Q1.6** Pour chacun des échanges de clés de chiffrement utilisés dans les différents cas suivants, lequel des trois termes de la question précédente est approprié ? (expliquer)

— connexion ssh
— connexion https avec autorité de certification
— chiffrement de mail par clé gpg

**Q1.7** Pour chacun de ces trois cas, pourquoi a-t-on choisi ce mode d'échange de clé ?

**Exercice 2.** Adresses

**Q2.1** Un fournisseur d'accès Internet aux États-Unis vient d'obtenir du RIPE la plage d'adresses IPv4 `185.233.100.0/22`. De combien d'adresse dispose-t-il ? Il veut la découper en sous-réseaux `/24`, combien cela en fait-il ? Est-ce que les adresses suivantes font partie du `/22` ? `185.233.101.1`, `185.233.99.254`, `185.233.105.100`, `185.233.100.105`, `185.233.112.100`,

**Q2.2** Il a également obtenu la plage d'adresses IPv6 `2a0c:e300::/32` , et observe que l'IETF recommande d'attribuer un `/56` à chacun de ses abonnés. Combien d'abonnés peut-il avoir ? Est-ce beaucoup ?

**Exercice 3.** Calculs (on pourra faire des arrondis de calculs grossiers si l'on ne dispose pas de calculatrice)

Je dispose d'une ligne ADSL 16Mbps/1Mbps. On négligera le surcoût des en-têtes des protocoles réseau utilisés.

**Q3.1** Je désire envoyer un fichier de 125Mo sur un site web, combien de temps devrai-je attendre ? Quelle est un ordre de grandeur de la latence pendant le transfert ?

**Q3.2** Mon voisin, ayant une ligne ADSL ayant la même vitesse, veut récupérer ce même fichier de 125Mo, combien de temps devra-t-il attendre ? Quelle est un ordre de grandeur de la latence pendant le transfert ?

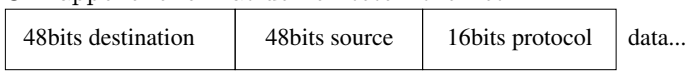
**Q3.3** Sachant que ma clé USB a un débit de 12,5Mo/s en écriture et 25Mo/s en lecture, et que je mets 5 minutes à aller à pied chez mon voisin, est-ce vraiment intéressant de passer par Internet pour s'échanger ce fichier de 125Mo ? Quel est un ordre de grandeur de la latence pendant le transfert ?

**Exercice 4.** Analyse de paquet

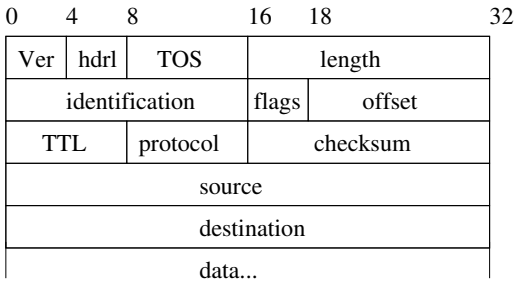
Voici un paquet IP capturé par *wireshark* :

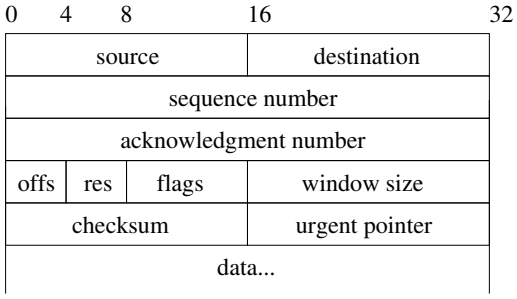
```
0000:  45 10 00 28 bb a2 40 00 40 06 1c 2c 0a 00 00 0e  E..4..@.@..,....
0010:  80 0a 0b 02 04 0a 00 16 9a e8 9b dd 42 4d 7d 5e  .....‘......BM}^
0020:  80 10 07 d4 a7 0c 00 00                          ........
```

On rappelle le format de l'en-tête Ethernet :




le format des en-têtes IPv4 et TCP :




**Q4.1** Que sont les adresses IP source et destination ?

**Q4.2** Quel est le numéro de port source et le numéro de port destination ? Combien de données applicatives sont transportées ? Que pouvez-vous en conclure ?

**Exercice 5.** Mosh

**Q5.1** Le protocole mosh propose de fournir le même service de connexion shell à distance que ssh, mais via UDP. L'idée est que `mosh-client` commence par établir une connexion ssh normale pour se connecter au serveur ssh, et ouvre à côté une socket UDP. Il fait lancer par le serveur le programme `mosh-server` qui ouvre sur le serveur une socket UDP. `mosh-client` et `mosh-server` s'échangent par la connexion ssh une clé de session, et peuvent alors échanger des datagrammes en UDP chiffrés avec la clé de session, ils referment alors la connexion ssh dont ils n'ont plus besoin : tout passe désormais par UDP.

Faites des dessins pour expliquer le déroulement de la connexion.

**Q5.2** Dans le sens serveur vers client, `mosh-server` n'envoie pas exactement ce que les programmes lancés à distance impriment : par exemple si une commande imprime beaucoup de texte, `mosh-server` n'est pas obligé de tout envoyer au client, il pourrait même envoyer seulement les 25 dernières lignes (en supposant que votre terminal fait 25 lignes). On veut tout de même pouvoir observer la progression, donc envoyer quand même 25 lignes de temps en temps. Comment choisir la fréquence à laquelle faire ces envois ?

**Q5.3** Que se passe-t-il si je perds mon accès internet pendant qu'un programme qui s'exécute sur le serveur imprime du texte, et que je ne récupère mon accès qu'une fois que le programme a fini d'imprimer du texte ? Quelle stratégie mosh doit-il utiliser pour avoir un résultat convenable ?

**Q5.4** Dans le sens client vers serveur, mosh est obligé d'assurer la transmission de la même façon qu'en TCP, pourquoi ?

**Q5.5** Est-ce que l'on peut utiliser de la même façon UDP pour remplacer le service scp de ssh ? Pourquoi ?