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 3 **pages**

université de BORDEAUX

Collège Sciences et technologie

Exercice 1. Questions de cours

Q1.1 Comme son acronyme l'indique, HTTP est le (P)rotocole qui (T)ransporte des pages web, alors que HTML est le (L)angage qui permet de décrire des pages web à l'aide de balises ((M)arkup).

Q1.2 Il faut absolument activer le support https, pour que le mot de passe ne soit pas envoyé en clair via Internet, permettant aux opérateurs sur le chemin de le lire.

Q1.3 Cela permet de séparer deux questions : routage et gestion de flux. Les routeurs d'Internet ne font que traiter la partie IP pour le routage, et ne se préoccupent pas de la gestion de flux, qui est gérée seulement par les extrêmités. Cela permet de construire des routeurs simples et efficaces.

Q1.4 25600 = 256*100, apparemment ils ne se sont pas mis d'accord sur l'ordre des deux octets de l'entier 16 bits, qui se sont retrouvés interprétés à l'envers, d'où la multiplication par 256. Il aurait fallu se mettre d'accord, et notamment utiliser la recommandation IETF qui est d'envoyer d'abord l'octet de poid le plus fort (big-endian).

Q1.5 Dans une organisation centralisée, tout passe par un seul centre, et lorsque celui-ci est en panne, plus rien en fonctionne.

Dans une organisation décentralisée, le centre délègue une partie de son fonctionnement à des sous-centres. Si le centre tombe en panne, des parties de l'organisation peuvent ainsi fonctionner en indépendance, l'absence du centre ne fait que dégrader le service fourni (par exemple des communications globales sont impossibles, seules les communications locales fonctionnent).

Dans une organisation acentrée, il n'y a pas de centre particulier. Si une machine tombe en panne, les services associés sont en panne, mais toutes les autres machines continuent de fonctionner correctement, contournant au besoin la machine en panne.

Q1.6

- connexion ssh
  Le fonctionnement est acentré : il n'y a pas de centre pour gérer les échanges de clés, c'est effectué directement entre le client et le serveur et entre l'utilisateur du client et l'administrateur du serveur. On a choisi ce mode d'échange pour pouvoir mettre en place un serveur ssh sans avoir à demander à qui que ce soit de le faire.
- connexion https avec autorité de certification
  La signature des clés est centralisé : c'est l'autorité de certification qui assure la certification. On peut par contre dire que la vérification décentralisée : le certificat de l'autorité étant installé au préalable sur les postes clients, ils peuvent vérifier eux-même le certificat du serveur, l'autorité n'est pas impliquée pour la vérification. Il faut par contre régulièrement mettre à jour le certificat de l'autorité, pour le cas où il serait révoqué par exemple.
  On a choisi ce mode d'échange pour ne pas nécessiter d'échange entre l'utilisateur du client et l'administrateur du serveur. Il y a seulement un échange entre l'administrateur du serveur et l'autorité de certification, et un échange entre l'autorité de certification et le mainteneur du navigateur web.
- chiffrement de mail par clé gpg
  Le fonctionnement est acentré : il n'y a pas de centre pour gérer les échanges de clés. On peut utiliser des serveurs de clés pour diffuser sa clé gpg, mais ce n'est pas obligatoire, on peut la déposer sur son site web, etc. La vérification est de toutes façons indépendante de la récupération de la clé.
  On a choisi ce mode d'échange pour les mêmes raisons que ssh : on ne veut pas avoir à demander à qui que ce soit pour pouvoir chiffrer des mails.

Exercice 2. Adresses

Q2.1
Il dispose de $2^{32-22} = 2^{10} = 1024$ adresses.
Cela fait $2^{24-22} = 2^2 = 4$ sous-réseaux /24.
`185.233.101.1` : oui, `185.233.99.254` : non, `185.233.105.100` : non, `185.233.100.105` : oui, `185.233.112.100` : non

Q2.2 Cela fait $2^{56-32} = 2^{24} = 16\,777\,216$ abonnés. Ce n'est pas tant que ça pour la France par exemple, pour les États-Unis c'est vraiment peu...

Exercice 3.

Q3.1 On envoie à 1Mbps, i.e. 0.125Mo/s. Il faut donc 1000 secondes pour envoyer 125Mo, soit un peu moins de 20 minutes.
La latence est celle de la ligne ADSL, environ 50 ms.

Q3.2 La récupération est à 16Mbps, donc 2Mo/s, il suffit donc de $125Mo/2Mo/s = 62.5s$ pour récupérer le fichier, donc environ 1 minute. La latence est la même.

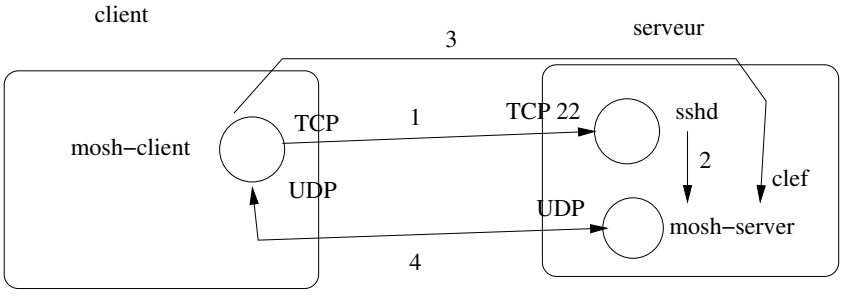
Q3.3 Il faut d'abord écrire sur la clé, à 12.5Mo/s, donc 10s pour écrire le fichier. Il faut ensuite 5 minutes pour marcher. On lit enfin la clé USB à 25Mo/S, donc 5s pour lire. Les transferts USB sont presque négligeables en fait, et 5 minutes c'est bien moins que les 20 minutes nécessaires pour le transfert par Internet.

Exercice 4.

Q4.1 10.0.0.14 et 128.10.11.2

Q4.2 1034 et 22.
0 octets
C'est probablement un simple acquittement vers un serveur ssh.

Exercice 5. Mosh



Q5.1
La connection ssh via TCP est représentée en 1. Le lancement de `mosh-server` est représenté en 2. L'échange de clef via ssh entre `mosh-client` et `mosh-server` est représenté en 3. La communication chiffrée entre `mosh-client` et `mosh-server` est représentée en 4.

Q5.2 On peut gérer le flux à la manière de TCP : on essaie d'envoyer des lignes de plus en plus souvent, jusqu'à ce que les acquittements venant du client commencent à manquer, ce qui signifie que l'on envoie trop souvent, on réduit alors la cadence d'envoi. De temps en temps, on essaie de nouveau d'envoyer plus souvent, pour le cas où le réseau était juste encombré temporairement.

Q5.3 Le serveur mosh est obligé de se souvenir des 25 dernières ligne, pour pouvoir les envoyer au client une fois l'accès rétabli.

Q5.4 On ne veut pas perdre les pressions de touches de l'utilisateur, ni les réceptionner dans le désordre ! (alors que pour l'affichage, c'est beaucoup moins un problème s'il se fait dans le désordre, tant que le résultat final des 25 lignes est correct).

Q5.5 scp doit envoyer le fichier complet et dans le bon ordre, on a donc besoin de toutes les garanties de TCP.