Année Universitaire 2022-2023 session 1 d'automne

Parcours : TAH Licence pro ADSILLH **UE :** 4TAH506U
Épreuve : Examen réseaux
Date : 18 novembre **Heure :** 14h00 **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 / discussions de cours

Q1.1 Que se passe-t-il précisément si je configure sur le même réseau deux machines avec la même adresse IP ?

Q1.2 Un collègue m'affirme que les transferts TCP garantissent l'intégrité des données. Dans quelle mesure TCP garantit-il vraiment l'intégrité ?

Q1.3 Expliquer pourquoi il peut être problématique de brancher 3 switchs les uns sur les autres, et ce qu'on peut utiliser pour éviter le problème.

Q1.4 Classez ces noms de fonction dans l'ordre d'utilisation typique : accept, close, listen, read, socket, write. Lequel d'entre eux prend en paramètre une socket *et* retourne une socket ? À quoi cela sert-il ?

Q1.5 Je récupère un fichier .zip depuis Internet. J'essaie de le décompresser sur mon ordinateur, mais les noms de fichiers sont bizarre. Par exemple, j'obtiens un fichier appelé « ÃchÃ©ancier.odt ». Quand je décompresse le même fichier zip sur un autre ordinateur, je n'ai pas de problème, j'obtiens un fichier appelé « Échéancier.odt ». Expliquer précisément ce qui se passe, pourquoi le comportement est différent sur les deux ordinateurs, et ce qui devrait se passer.

Exercice 2. Adresses

On installe un réseau dans une résidence étudiante comportant 300 chambres. On utilise pour cela le réseau IPv4 `10.0.0.0/23`

Q2.1 Pourquoi ce réseau est-il suffisamment grand ? Quelles sont les adresses effectivement utilisables ?

Q2.2 Finalement on utilise plutôt des réseaux séparés pour les 4 bâtiments de la résidence, qui sont de tailles similaires. Indiquez quels sous-réseaux IPv4 on peut utiliser pour cela.

On ajoute IPv6 aux réseaux de la résidence. On dispose du réseau `2001:0db8:1234::/48` pour l'ensemble de la résidence, qui est composée des bâtiments 1, 2, 3 et 4.

Q2.3 Quels sous-réseaux IPv6 utiliser pour chaque bâtiment, en allant au plus simple ?

Exercice 3. Calculs (on pourra faire des arrondis de calculs grossiers si l'on n'a pas de calculatrice). Précisez le déroulement de votre calcul.

Q3.1 J'ai une image de disque dur de VM de 7 Go à transférer d'un poste à l'autre du cremi. Le réseau est câblé en gigabit Ethernet. Combien de temps le transfert mettra-t-il ?

Q3.2 Je constate que le transfert est bien plus lent que cela. Qu'est-ce qui pose le plus probablement problème ?

Q3.3 Combien de paquets ont été transmis pendant le transfert ?

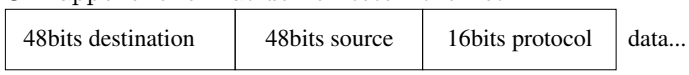
Q3.4 Supposons que le réseau a une latence de 100µs. Si TCP n'envoyait qu'un seul paquet en avance, attendant donc de recevoir l'acquittement du paquet n avant d'envoyer le paquet $n+1$, combien de temps le transfert mettrait-il ?

Exercice 4. Analyse de paquet

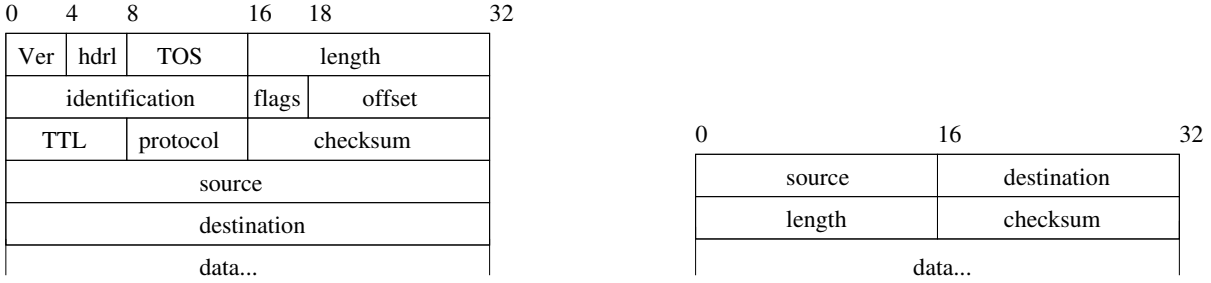
Voici une trame Ethernet capturée par *wireshark*, reçue par la carte réseau de mon ordinateur portable, pour un échange NTP (qui utilise UDP) :

```
0000|  b8 26 6c 59 6a 78 dc 41 a9 47 ec 49 08 00 45 b8   .&lYjx.A.G.I..E.
0010|  00 4c b7 8d 40 00 40 11 eb 06 0a 00 00 19 33 4d   .L..@.@.......3M
0020|  59 ef 00 7b 00 7b 00 38 97 9e 23 00 00 20 00 00   Y..{.{.8..#.. ..
0030|  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040|  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050|  00 00 06 37 08 ec bd 46 2a b5                     ...7...F*.
```

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



le format des en-têtes IPv4 et UDP :



Q4.1 Quelle est l'adresse IP de la machine envoyant le paquet ? Quel est le port utilisé du côté de l'émetteur, et de la destination ? Qu'est-ce qui est surprenant ?

Q4.2 Quelle est la taille en octets des données applicatives NTP ?

Exercice 5. Authentification SSH par certificats

Q5.1 Expliquer le principe TOFU et quel défaut il comporte.

Depuis quelques années, il est possible d'utiliser des certificats pour l'authentification SSH, plutôt que de simples clés utilisées couramment [1].

Q5.2 Rappelez brièvement le principe d'authentification par certificat avec autorité de certification.

Q5.3 Pour quelle raison utilise-t-on cela pour HTTPS ?

Q5.4 Pour quel genre de situation peut-il être souhaitable d'utiliser des certification pour l'authentification SSH du serveur par le client ? Comment pourrait-on gérer la distribution des certificats dans ce cas ?

Q5.5 Même question pour l'authentification SSH du client par le serveur.

1. Voir `https://lwn.net/Articles/913971/`