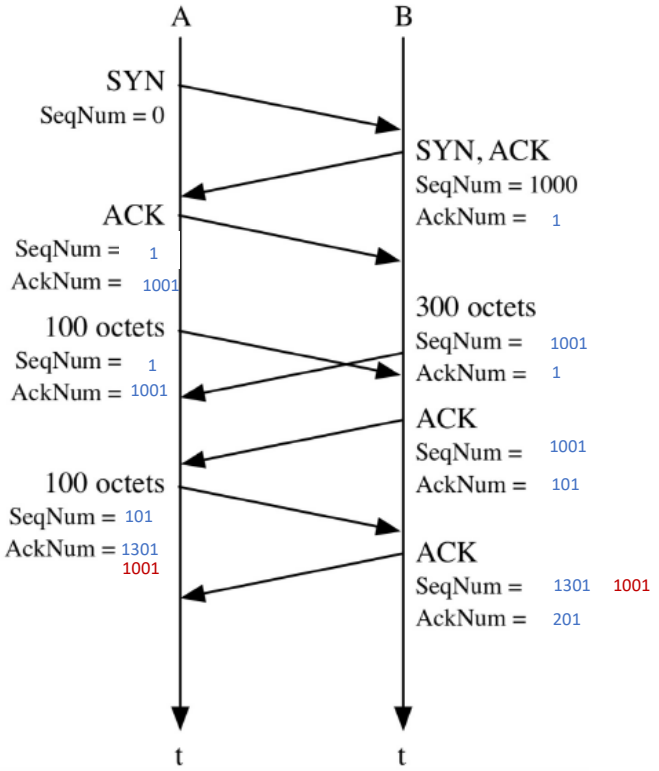
CR TP1

Lundi 22/02/2021

EI2I3-IIA **Julian BARKOUDEH**

Table des matières

1) Numeration de TCP



Premier cas

Deuxième cas

- Premier cas :
  - Transfert de A vers B : Tout d'abord, A initialise la connexion donc l'acquittement de B passe à 1. Ensuite, à la troisième ligne on remarque que l'acquittement passe à 101, ce qui confirme la réception d'un paquet de 100 octets. Dans le dernier ligne, l'acquittement passe à 201 pour confirmer le deuxième paquet.
  - Transfert de B vers A : On remarque qu'à la quatrième opération, le numéro de séquence de A passe à 101, reprenant l'acquittement de B de 101. Ainsi, l'acquittement passe à 1301, pour indiquer la réception du paquet de 300 octets.
- Deuxième cas :

  Comme le paquet de 300 octets est perdu, l'acquittement de A ne change pas, donc le numéro de séquence de B pour la dernière opération reste à 1001 aussi car celui-ci est lié à l'acquittement de A pour sa dernière opération.

2) Analyses manuelles

```
00 01 02 a5 fb 3a 00 01 02 a5 fc 8d 08 00 45 00
00 3c ec 26 40 00 40 06 cc cd 0a 21 b6 b6 84 e3
3c 0d 0e b5 00 50 a9 55 92 64 00 00 00 00 a0 02
3e bc a3 74 00 00 02 04 05 b4 04 02 08 0a 08 39
91 16 00 00 00 00 01 03 03 00
```

1) Nous pouvons récupérer « 00 01 02 a5 fb 3a » comme l'adresse destination, et l'adresse source « 00 01 02 a5 fc 8d ». Ainsi le type de données qui est « 08 00" qui correspond à un datagramme IP.
2) En se basant sur le schéma d'un datagramme IP dans les annexes, on peut définir les octets de la manière suivante :
   Version : « 4 »
   IHL : « 5 »
   TOS : « 00 »
   Total length : « 00 3c »
   Identification : « ec 26 »
   Flags : « 4 »
   Fragment offset : « 0 00 »
   TTL : « 40 »
   Protocol : « 06 »
   Header chercksum : « cc cd »
   Souce : « 0a 21 b6 b6 »
   Destination : « 84 e3 3c 0d »
3) D'après le IHL on déduit que l'entête sera de 5 mots de 32 bits donc 20 octets. Or on compte 20 octets jusqu'à l'adresse destination, donc il n'y a pas d'options.
4) **Source** : « 0a 21 b6 b6 »
   Destination : « 84 e3 3c 0d »
5) On identifie l'octet « 06 » comme le protocole. Donc il s'agit de la partie TCP.

6) **Source port** : « 0e b5 »
Destination port : « 00 50 »
Squence Number : « a9 55 92 64 »
Acknowledgment Number : « 00 00 00 00 »
Data offset : « a »
Reserved : « 0 »
URG : « 0 »
ACK : « 0 »
PSH : « 0 »
RST : « 0 »
SYN : « 1 »
FIN : « 0 »
Window : « 3e bc »
Checksum : « a3 74 »
Data : « 00…….. 03 00 »

3) Introduction Wireshark

4) HTTP

1) Ceci est une recurète pour obtenir la page BCI_exemple.html. Nous pouvons confirmer cela par la deuxième requête qui confirme la réception de la demande d'obtenir la page.
2) En regardant la troisième requête, on remarque que le type de donnée demandé est une image située sur un autre site.
3) La première requête envoyée est donc pour récupérer la page qui ne contient que du texte. Ensuite une requête est envoyée afin d'obtenir l'image de l'autre site. La page contenant le texte et l'image est ensuite affichée à l'utilisateur.
4) On identifie 3 machines d'adresses IP : 137.194.164.14, 137.194.2.8, 137.194.2.39
137.194.164.14 correspond à l'utilisateur, 137.194.2.8 à la page avec que du texte et, 137.194.2.39 à la page avec l'image.

5)

Seq = 1 Ack = 1

Seq = 1 Ack = 608

Seq = 1 Ack = 1

Seq = 2897 Ack = 499

On remarque que l'acquittement passe à la deuxième ligne à 608 pour affirmer la réception du paquet de 607 octets. En suite on remarque que l'acquittement passe à 499 pour confirmer la réception du paquet de 498 octets correspondant à l'image. Pour les 3 premiers lignes nous sommes dans la machine 2 et la dernière ligne pour la machine 3.

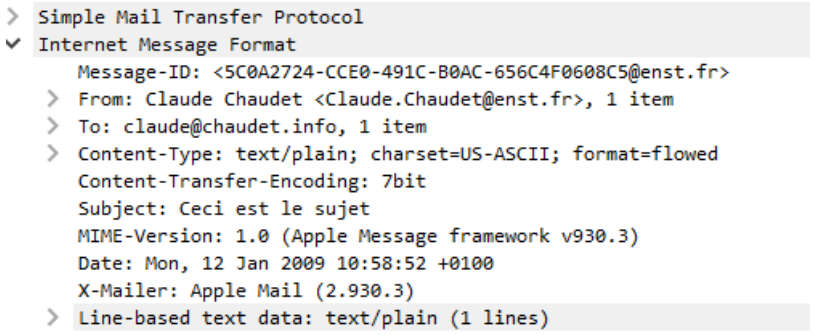
5) SMTP

1) En observant le premier échange, on observe le code 220. Ce code correspond au premier message envoyé par le serveur après l'établissions de la connexion. Donc c'est le serveur qui contacte le client au début.
On en déduit que :

Source : 137.194.2.14 Ce qui correspond au serveur

Destination: 137.194.164.14

2) Le sujet est spécifié par l'utilisation de « Subject : » de la façon suivante :
   Subject : « et on écrit le sujet du mail ».
3) On peut envoyer le message à plusieurs personnes en utilisant « RCPT TO : » .
4) En sélectionnant l'avant dernier trame, celui qui correspond au message total et en regardant le « Internet message format » nous pouvons visualiser le message tant qu'il est envoyé. On observe dans le premier cas que nous pouvons voir les personnes en copie, alors dans le deuxième cas nous pouvons plus les visualiser.



6) FTP

1) On remarque que le port 21 est utilisé.
2) Oui, on remarque la requête Quit par l'utilisateur.
3) ID : ftp, mot de passe : claude chaudet.
4) Une des risques c'est que nous pouvons visualiser le mot de passe et le nom d'utilisateur sur la trame.