

Protocoles réseaux

TD n° 7 : Traces de paquets

Exercice 1 :

1. Identifiez le nom de l'interface réseau par laquelle vous êtes connectés à l'Internet. (Sous Linux, vous pouvez par exemple utiliser la commande « `ip route show` pour déterminer l'interface par laquelle passe la route par défaut.)
2. Lancez la commande « `tcpdump -n -i interface` », où *interface* est l'interface déterminée ci-dessus. Pendant que `tcpdump` s'exécute, chargez une page *web*. Que se passe-t-il ?
3. Lancez *Wireshark*. Dans la page d'accueil de Wireshark, choisissez l'interface déterminée ci-dessus. Lancez la capture, puis téléchargez une page *web*. Que se passe-t-il ?

Exercice 2 :

Téléchargez le fichier

<https://www.irif.fr/~jch/enseignement/reseaux/trace.pcap>

et examinez-le, d'abord à l'aide de la commande « `tcpdump -n -r fichier` », ensuite à l'aide de « `tcpdump -r fichier` », enfin à l'aide de *wireshark*.

1. Quelles sont les adresses des interfaces qui communiquent ?
2. Quel protocole de couche transport est-il utilisé ?
3. Pourquoi autant de paquets ont-ils taille 1448 ?
4. Y a-t-il eu des pertes de paquet ?
5. Pourquoi autant de ack 118 ?
6. Pourquoi les numéros de séquence des deux premiers paquets sont énormes, et ceux des suivants petits ?
7. Au fait, quel est le nom des hôtes qui communiquent ?
8. Interpréter les *flags* (lettre entre crochets comme [S.])
9. Vers la fin on dirait qu'il y a moins de ack. Pourquoi ?
10. Interprétez les champs `val` et `ecr`.
11. Sur quel hôte la trace a-t-elle été capturée ? Justifier.

Exercice 3 :

Que se passe-t-il dans les fragments de traces suivants ? Toutes les traces ont été capturées sur la machine « A » (comment peut-on le voir ?).

1.

```
22:45:26.121149 A.32769 > B.www: S 2919412148:2919412148(0) win 5840
<mss 1460,nop,wscale 1>
22:45:26.123055 B.www > A.32769: S 4144006771:4144006771(0)
ack 2919412149 win 65535
<mss 1460,nop,wscale 1>
22:45:26.123120 A.32769 > B.www: . ack 1 win 2920
22:45:26.124144 A.32769 > B.www: P 1:146(145) ack 1 win 2920
22:45:26.130323 B.www > A.32769: . 1:1461(1460) ack 146 win 32850
22:45:26.130402 A.32769 > B.www: . ack 1461 win 4380
22:45:26.130750 B.www > A.32769: . 1461:2921(1460) ack 146 win 32850
```

2.

```
22:45:26.195481 B.www > A.32769: . 74461:75921(1460) ack 146 win 32850
22:45:26.196216 B.www > A.32769: P 75921:77381(1460) ack 146 win 32850
22:45:26.196228 A.32769 > B.www: . ack 77381 win 64240
22:45:26.211281 B.www > A.32769: . 77381:78841(1460) ack 146 win 32850
22:45:26.211772 B.www > A.32769: P 78841:80301(1460) ack 146 win 32850
22:45:26.211783 A.32769 > B.www: . ack 80301 win 64240
```

3.

```
22:45:26.240764 B.www > A.32769: P 127021:128387(1366) ack 146 win 32850
22:45:26.240776 A.32769 > B.www: . ack 128387 win 64240
22:45:26.249437 A.32769 > B.www: F 146:146(0) ack 128387 win 64240
22:45:26.251418 B.www > A.32769: . ack 147 win 32850
22:45:26.251840 B.www > A.32769: F 128387:128387(0) ack 147 win 32850
22:45:26.251871 A.32769 > B.www: . ack 128388 win 64240
```

4.

```
22:49:22.739301 A.32775 > C.ssh: . 110064:111524(1460) ack 2336 win 5104
22:49:22.739312 A.32775 > C.ssh: . 111524:112984(1460) ack 2336 win 5104
22:49:22.772816 C.ssh > A.32775: . ack 96924 win 62780
22:49:22.772828 A.32775 > C.ssh: . 112984:114444(1460) ack 2336 win 5104
22:49:22.772838 A.32775 > C.ssh: . 114444:115904(1460) ack 2336 win 5104
22:49:22.773905 C.ssh > A.32775: . ack 99844 win 62780
```

5.

```
22:53:47.759896 D.17775 > A.32782: . 75921:77381(1460) ack 1 win 17520
22:53:47.760031 D.17775 > A.32782: . 77381:78841(1460) ack 1 win 17520
22:53:47.760055 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885001 D.17775 > A.32782: . 80301:81761(1460) ack 1 win 17520
22:53:47.885072 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885816 D.17775 > A.32782: . 83221:84681(1460) ack 1 win 17520
22:53:47.885834 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885951 D.17775 > A.32782: . 84681:86141(1460) ack 1 win 17520
22:53:47.885962 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.917054 D.17775 > A.32782: . 86141:87601(1460) ack 1 win 17520
22:53:47.917065 A.32782 > D.17775: . ack 78841 win 64240
22:53:48.042369 D.17775 > A.32782: . 78841:80301(1460) ack 1 win 17520
22:53:48.042419 A.32782 > D.17775: . ack 81761 win 64240
22:53:48.199537 D.17775 > A.32782: . 81761:83221(1460) ack 1 win 17520
22:53:48.199602 A.32782 > D.17775: . ack 87601 win 64240
22:53:48.199718 D.17775 > A.32782: . 89061:90521(1460) ack 1 win 17520
22:53:48.199732 A.32782 > D.17775: . ack 87601 win 64240
22:53:48.356490 D.17775 > A.32782: . 87601:89061(1460) ack 1 win 17520
22:53:48.356551 A.32782 > D.17775: . ack 90521 win 64240
22:53:48.356620 D.17775 > A.32782: . 90521:91981(1460) ack 1 win 17520
```

Exercice 4 :

Que se passe-t-il sur chacun des diagrammes temps-séquence suivants ?



