Réseaux sans fil avancé

Prénom et nom :

_____

_____

Informations générales

Dans ce laboratoire, vous allez travailler individuellement. Le travail devrait se faire en deux séances.

Rapport : Un rapport individuel devra être rendu deux semaines de cours après le labo.

Introduction

Ceci est la suite du laboratoire Wireshark que vous avez déjà fait. Ici, nous allons analyser d'autres aspects de trames 802.11.
La capture de paquets dans les réseaux 802.11 requiert en général de hardware supplémentaire puisque l'accès aux cartes intégrées aux Laptops est limité. Il faut pour cette raison utiliser des cartes externes spécialisées connectées à votre machine par le port USB.
Pour s'adapter aux recommandations concernant la situation sanitaire actuelle, ce laboratoire utilise un fichier contenant des captures déjà faites qui est mis à disposition par le personnel enseignant.
Les captures dans le fichier ont été effectuées dans un réseau basé sur infrastructure.

Informations sur les adresses utilisées dans les trames 802.11 :
Notez que dans l'entête des trames 802.11, il y a jusqu'à 4 adresses :

SA (Source Address)	Adresse de la station ou AP qui a généré la trame.
DA (Destination Address)	Adresse de la destination finale (station ou AP)
TA (Transmitter Address)	Adresse de la station ou AP qui va effectuer la transmission de la trame ou, si elle est dans l'air, de la station ou AP qui vient de la transmettre.
RA (Receiver Address)	Adresse de la station ou AP proche qui va recevoir la trame en ce moment.

Les trames contiennent une, deux ou trois de ces adresses dans leur entête. Seule les trames qui circulent par le DS entre les APs utilisent les quatre.

Partie 1

Questions

Utilisez l'Internet pour trouver des réponses aux questions suivantes sur la capture de trames 802.11 :

1. Qu'est-ce que le mode monitor ?

.....

.....

.....

2. Qu'est-ce que le mode promiscuous ?

.....

.....

.....

3. Qu'est-ce que les cartes Alfa ?

.....

.....

.....

4. Qu'est-ce que aircrack-ng ?

.....

.....

.....

5. Que font les commandes de ligne suivantes ?

a. airmon-ng

.....

.....

.....

b. airodump-ng

.....

.....

.....

Partie 2

Caractérisation du réseau

Le réseau pour lequel vous devez analyser les trames est fomé de deux stations et un AP.

6. Cherchez l'adresse MAC de l'AP.

……

7. Cherchez des infos sur la version du réseau (Radiotap ?)

……

8. Cherchez des pings (ICMP) et déterminez :

a. Les adresses IP des chacune des stations

……

……

b. Les adresses MAC de chacune des stations

……

……

Partie 3

Filtres Wireshark avancés

Comme vous avez vu u dernier labo, les réseaux sans fil 802.11 peuvent être très « bavards ». Vous avez déjà trouvé et utilisé un filtre pour ne pas afficher les trames beacon. Nous allons créer d'autres filtres dans ce laboratoire.

Chercher et notez les filtres suivants (vous allez très probablement les utiliser dans ce labo) :

9. Donner le filtre pour ne voir que les transmissions depuis ou vers une adresse IP spécifique

.....

10. Appliquez le filtre à la capture dans le fichier Capture ADR.pcapng que vous avez utilize au dernier laboratoire en utilisant l'adress IP de la station qui transmettait les pings et montrez une capture d'écran où on puisse voir le filtre est le résultat.

11. Avec le filtre que vous avez créé pour la question 1, les trames ACK ne sont plus affichées. Pourquoi ?

.....

.....

12. Créez un filtre qui permette d'afficher toutes les trames transmises par la une des stations (y compris les ACK, RTS et CTS).

.....

13. Appliquez le filtre à la capture et montrez une capture d'écran (on devrait y voir ACK, RTS et CTS éventuels).

14. Créez un filtre pour ne montrer que les trames de contrôle :

.....

15. Créez un filtre pour ne montrer que les trames RTS

.....

16. Créez un filtre pour ne montrer que les trames CTS

.....

17. Créez un filtre pour ne montrer que les trames ACK

.....

Pour mieux comprendre les filtres suivants sur les adresses TA, RA, SA, et DA, voir explication à l'introduction de cette donnée de labo.

18. Créez un filtre pour ne voir que les trames avec une transmitter address (TA) donnée

.....

19. Créez un filtre pour ne voir que les trames ACK transmises par l'AP.

.....

20. Créez un filtre pour ne voir que les trames de données transmises soit par une des stations, soit par l'autre (mais pas par l'AP) et montrez une capture d'écran.

.....

Partie 4

Captures

a. CSMA/CA unicast d'une STA à une autre sans fragmentation

21. Dessinez la séquence de trames qui correspond à une transmission unicast utilisant la méthode CSMA/CA sans fragmentation dans un réseau basé sur infrastructure.

Dans le fichier .pcapng que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée.

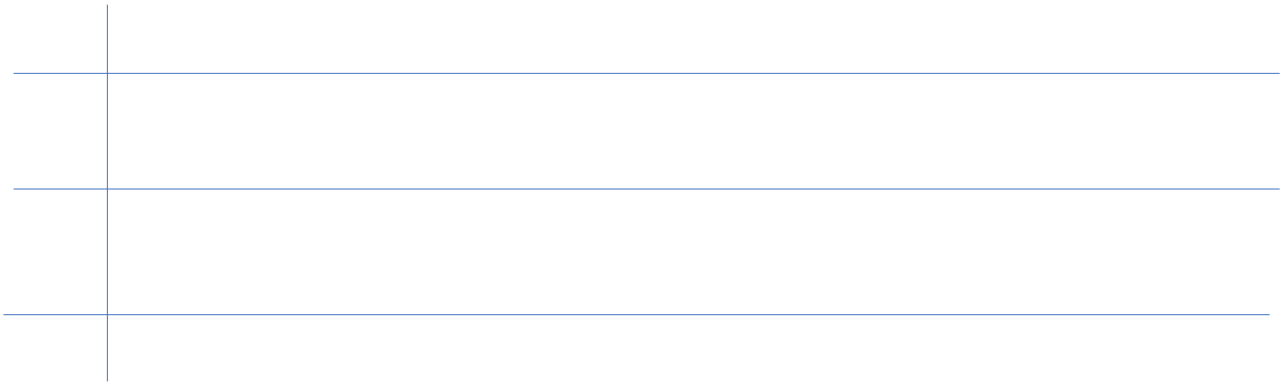
Attention : Notez que les transmissions entre une station et l'AP et entre l'AP et une autre station sont indépendantes en ce sens qu'il peut y avoir beaucoup de trafic entre les deux transmissions. Vous devriez pouvoir trouver les deux transmissions, mais pas forcément l'une suivie immédiatement par l'autre.

22. Collez une ou deux captures d'écran et donnez les informations suivantes sur les trames :

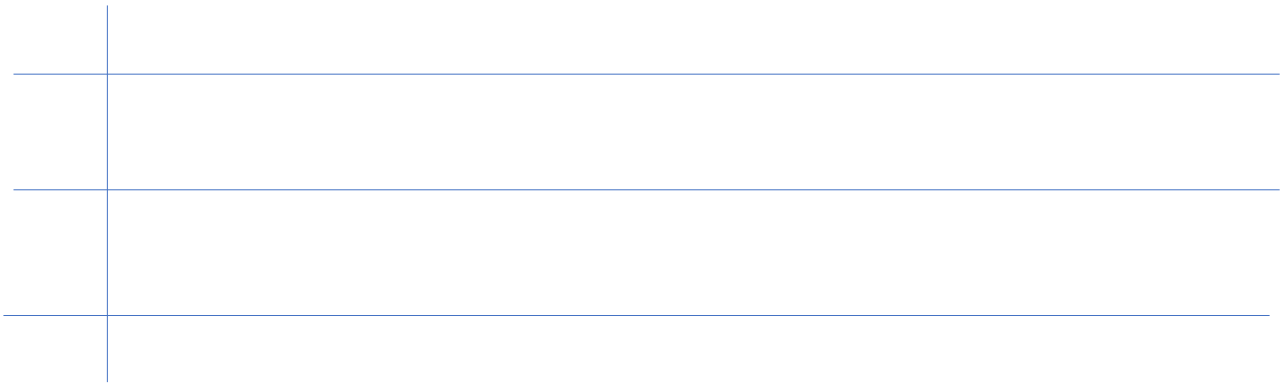
Numéro de la trame	Qui transmet (STA1, AP, STA2)	Qui reçoit (STA1, AP, STA2, Broadcast)	Type de trame (Données, ACK, RTS/ CTS, autre)

b. CSMA/CA unicast d'une STA à une autre avec fragmentation des trames transmises par l'AP

23. Dessinez la séquence de trames qui correspond à une transmission unicast utilisant la méthode CSMA/CA dans un réseau basé sur infrastructure avec fragmentation des trames transmises par l'AP.



Continuation si nécessaire…



Dans le fichiers .pcapng que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée.

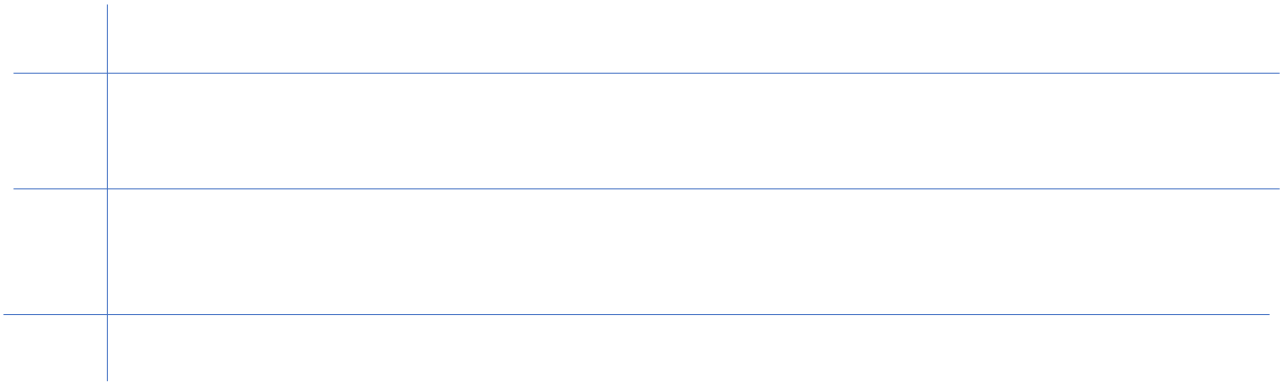
Attention : Notez que les transmissions entre une station et l'AP et entre l'AP et une autre station sont indépendantes en ce sens qu'il peut y avoir beaucoup de trafic entre les deux transmissions. Vous devriez pouvoir trouver les deux transmissions, mais pas forcément l'une suivie immédiatement par l'autre.

24. Collez une ou deux captures d'écran et donnez les informations suivantes sur les trames :

Numéro de la trame	Qui transmet (STA1, AP, STA2)	Qui reçoit (STA1, AP, STA2, Broadcast)	Type de trame (Données, ACK, RTS/ CTS, autre)

c. RTS/CTS unicast d'une STA à une autre sans fragmentation

25. Dessinez la séquence de trames qui correspond à une transmission unicast utilisant la méthode RTS/CTS sans fragmentation dans un réseau basé sur infrastructure.



Dans le fichiers .pcapng que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée.

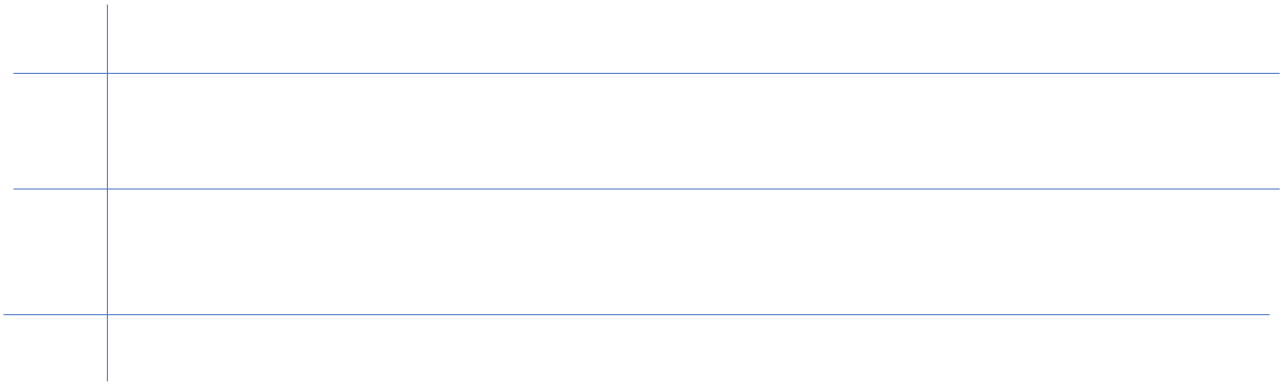
Attention : Notez que les transmissions entre une station et l'AP et entre l'AP et une autre station sont indépendantes en ce sens qu'il peut y avoir beaucoup de trafic entre les deux transmissions. Vous devriez pouvoir trouver les deux transmissions, mais pas forcément l'une suivie immédiatement par l'autre.

26. Collez une ou deux captures d'écran et donnez les informations suivantes sur les trames :

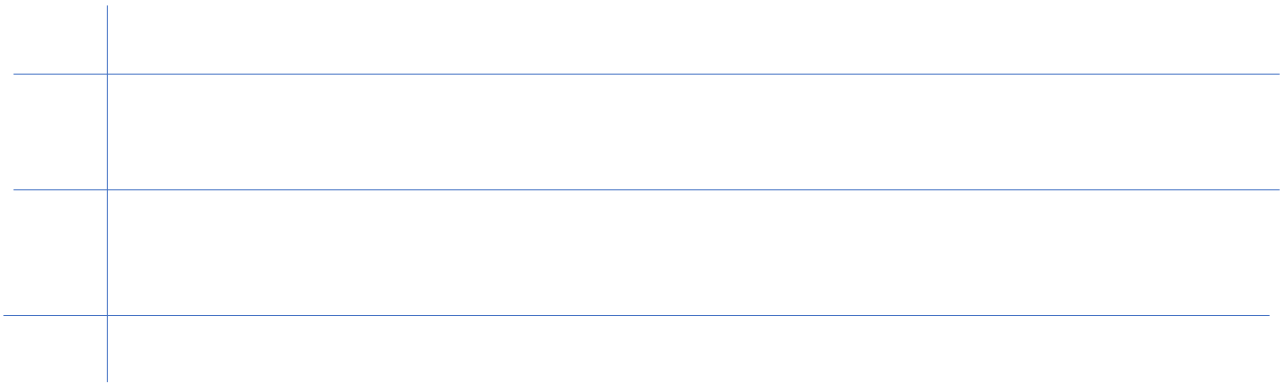
Numéro de la trame	Qui transmet (STA1, AP, STA2)	Qui reçoit (STA1, AP, STA2, Broadcast)	Type de trame (Données, ACK, RTS/ CTS, autre)

d. RTS/CTS unicast d'une STA à une autre avec fragmentation des trames transmises par l'AP

27. Dessinez la séquence de trames qui correspond à une transmission unicast utilisant la méthode RTS/CTS avec fragmentation dans un réseau basé sur infrastructure avec fragmentation des trames transmises par l'AP.



Continuation si nécessaire…



Dans le fichiers .pcapng que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée.

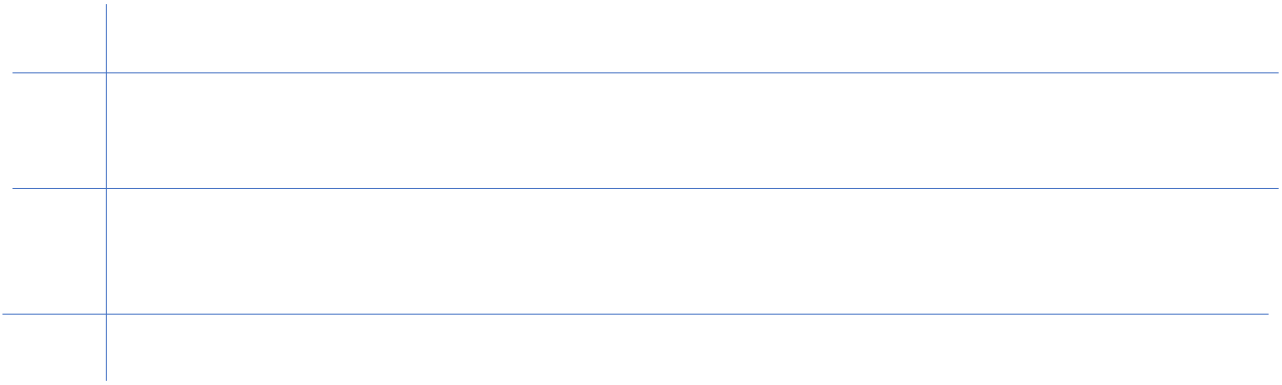
Attention : Notez que les transmissions entre une station et l'AP et entre l'AP et une autre station sont indépendantes en ce sens qu'il peut y avoir beaucoup de trafic entre les deux transmissions. Vous devriez pouvoir trouver les deux transmissions, mais pas forcément l'une suivie immédiatement par l'autre.

28. Collez une ou deux captures d'écran et donnez les informations suivantes sur les trames :

Numéro de la trame	Qui transmet (STA1, AP, STA2)	Qui reçoit (STA1, AP, STA2, Broadcast)	Type de trame (Données, ACK, RTS/ CTS, autre)

e. CSMA/CA broadcast depuis une STA et sans fragmentation

29. Dessinez la séquence de trames qui correspond à une transmission broadcast depuis une station utilisant la méthode CSMA/CA sans fragmentation dans un réseau basé sur infrastructure. Vous pouvez par exemple trouver les trames associées au protocole ARP.



Dans le fichiers .pcapng que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée.

Attention : Notez que les transmissions entre une station et l'AP et entre l'AP et une autre station sont indépendantes en ce sens qu'il peut y avoir beaucoup de trafic entre les deux transmissions. Vous devriez pouvoir trouver les deux transmissions, mais pas forcément l'une suivie immédiatement par l'autre.

30. Collez une ou deux captures d'écran et donnez les informations suivantes sur les trames :

Numéro de la trame	Qui transmet (STA1, AP, STA2)	Qui reçoit (STA1, AP, STA2, Broadcast)	Type de trame (Données, ACK, RTS/ CTS, autre)

f. Retransmissions

31. Trouvez une trame pour laquelle le ACK n'est pas arrivé et qui a été retransmise. Montrez le filtre que vous avez utilisé et montrez une capture d'écran.

---

g. Bonus

32. Trouvez le temps de transmission d'un CTS en utilisant les champs « Duration » des trames RTS et CTS successives at les informations qui se trouvent dans les normes (c'est dire, le SIFS, DIFS, Slot).