**Analyse de réseaux sans fil**

Prénom et nom :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Informations générales

Même si le labo est à rendre par équipes de trois élèves (voir prochain paragraphe sur le rapport), vous allez travailler individuellement. Les questions posées seront évaluées au deuxième TE. Pour cette raison, devrez connaître et comprendre les questions et leurs réponses. Le travail devrait se faire en deux séances. Les questions marquées avec l’icone  seront évaluées au TE.

**Rapport :**

Un rapport sera soumis par équipe de 3 élèves. Vous pouvez communiquer par Teams ou par email pour travailler sur le rapport mais, si ce n’est pas encore fait, chaque élève doit installer Wireshark individuellement.

**Attention : Le rapport doit être rendu au format pdf (pas manuscrit ni docx). Vous pouvez utiliser le fichier Word mis à disposition et le convertir en PDF avant de l’envoyer.**

Le rapport est dû à 18:00 le 19.1.2024 par email adressé à l’assistante (magali.egger@heig-vd.ch) avec copie au professeur (marcos.rubinstein@heig-vd.ch).

# Introduction

**Informations sur les adresses utilisées dans les trames 802.11 :**

Un des objectifs de ce laboratoire est de comprendre l’utilisation de 4 types d’adresses et autres informations qui apparaissent dans l’entête des trames 802.11.

Cette introduction présente une analogie sur les 4 types d’adresses. Elle comntient également des informations sur la signification de ces 4 adresses dans les réseaux WiFi. Une partie des exercices que vous allez faire au cours de ce laboratoire vous aidera à comprendre comment ces adresses sont utilisées.

**Analogie :**

Dans un réseau 802.11 basé sur infrastructure, une trame transmise par une station STA1 vers une autre station STA2 doit passer par un AP. La situation est similaire à celle de deux trains de marchandises. Regardez la figure ci-dessous



Fig. 1. Analogie des trains pour expliquer les 4 différentes adresses : la SA, la DA, la TA et la RA. Les maisonnettes représentent des gares.

- Les données sont comme des marchandises transportées par train.

- Yverdon (STA1) envoie un train à Morges (AP), où les marchandises sont transférées sur un autre train.

- Le deuxième train part de Morges vers Genève (STA2), qui est la destination finale.

Les trains dans l’analogie représentent des trames de données.

En dessus de chaque train dans la figure, il y a une description des adresses qui doivent être connues pour que le train arrive à bon port. Il y a 4 adresses : DA, SA, TA et RA. Voici une explication de la signification de chacune de ces adresses :

1. La SA (Source Address en anglais) indique le point de départ des marchandises (données). Notez que le point de départ des marchandises n’est pas forcément égal au point de départ du train en question. En effet, dans le cas du train au départ de Morges, le point de départ des marchandises (données) et toujours Genève, mais si le point de départ du train qui les transporte est Morges.
2. La DS (Destination Address en anglais) indique la destination finale. Dans ce cas aussi, il faut faire la distinction entre le point de destination du train et le point de destination des marchandises (données). En effet, les marchandises (données) transportées par le train entre Yverdon et Morges ont comme adresse de destination Genève, même si le point de destination du train est Morges.

Vous pouvez voir donc que, puisque ces deux adresses se réfèrent aux marchandises transportées par les trains, elles sont indépendante du train en question :

Pour le train au départ Yverdon, SA=Yverdon et DA=Genève et pour le train au départ de Morge elles restent inchangées, SA=Yverdon et DA=Genève.

La situation est différente pour les adresses TA et RA

1. La TA (Transmitter Address en anglais) représente le point de départ du train et non pas le point de départ des marchandises (données). Pour le train d’Yverdon à Morges, la TA est donc Yverdon mais pour le train entre Morges et Genève, la TA est Morges.
2. La RA (Receiver Address en anglais) identifie la destination du train et ne doit pas être confondi avec la destination des marchandises (données). Pour le train entre Yverdon et Morges, la TA est donc Morges mais pour le train entre Morges et Genève, la RA est Genève.

Nous avons déjà mentionné que les trains représentent des trames transportant des données. Notez que dans notre analogie (ls analogies ne sont généralement pas parfaites), les trames ACK ne sont pas représentées.

Revenons maintenant au réseaux WiFi.

Les 4 types d’adresse expliquées précédemment sont utilisées dans les trames transmises dans les réseaux 802.11 mais pas toutes les adresses sont présentes dans toutes les trames. En effet, certaines trames ne contiennent dans leur entête qu’une seule de ces adresses. C’est le cas des trames ACK et CTS dans lesquelles on retrouve seulement la RA. D’autres trames en deux des adresses dans leur entête, comme dans le cas de la trame RTS qui ne contiennent que les adresses TA et RA. Encore d’autres trames ont dans leur entête trois adresses. C’est le cas pour les trames de données.

Voici encore une fois les quatre adresses utilisées dans 802.11 :

Tabelle 1. Quatre adresses utilisées dans 802.11.

|  |  |
| --- | --- |
| SA (Source Address) | Adresse MAC de l'expéditeur d'origine des données. Indique d’où les données proviennent. |
| DA (Destination Address) | Adresse MAC de la destination finale des données. |
| TA (Transmitter Address) | Adresse MAC de la station qui a transmis la trame.  |
| RA (Receiver Address) | Adresse MAC de la station qui reçoit la trame.  |

## Partie 1

*Adresse MAC, SSID et BSSID*

Le réseau que nous allons analyser comprend deux stations STA1 et STA2 connectées à un point d'accès (AP).



Fig. 2. Le réseau à analyser dans ce labo, composé d’un AP et de deux stations, que nous appellerons STA1 et STA2.

Les réseaux basés sur infrastructure ont deux identifiants. Le premier est composé de caractères lisibles (de lettres ou/et des chiffres). Cet identifiant s’appelle SSID. Des exemples de SSID sont « heig-vd », «Starbucks » et « chouchou ».

Le deuxième identifiant s’appelle BSSID ou BSS id et il est composé de 6 octets représentés en hexadécimal.

Le SSID du réseau que nous allons analyser a « LaboLAN » comme SSID et son BSSID est 20:aa:4b:56:5a:e1.

Le BSSID (celui qui est unique au monde) est ce qu’on appelle une adresse MAC que vous avez déjà vue quand nous avons étudié les réseaux Ethernet. Les adresses MAC ne sont pas seulement utilisées pour identifier les réseaux sans fil 802.11. Elles identifient en fait toutes les cartes réseau. Nuas avons déjà vu ces adresses dans les réseaux Ethernet. Vous pouvez regarder cette vidéo courte qui explique de manière succincte l’utilisation des adresses MAC : <https://www.youtube.com/watch?v=s65VWFzVuMg>

Nous avons évoqué plusieurs types de trames telles les trames ACK, les trames CTS, les trames RTS et les trames de données. Cependant, nous n’avons pas encore mentionné la trame beacon qui est la trame la plus fréquente dans les réseaux WiFi puisqu’elle est transmise par l’AP dix fois par seconde. La trame beacon contient le SSID.

En ce qui suit, les questions seront posées à l’intérieur de cadres avec arrière-plan bleu.

Le fichier de capture Wireshark fourni avec ce labo contient de nombreux échanges de trames dans plusieurs réseaux. Chaque réseau est identifié par son SSID qui est transmis dans les trames beacon.

1. Ouvrez le fichier « Capture Labo RSE.pcapng » avec Wireshark et utilisez un filtre pour ne voir que les trames beacon. Vous pouvez trouver le filtre sur internet effectuant par exemple une recherche sur Google avec les mots 802.11 wireshark filters. Observez ensuite dans la colonne Info dans Wireshark les différents SSID. Vous y verrez par exemple SSID= ”public-HEIG-VD”. Chaque SSID indique la présence d’un réseau différent. Montrez une capture d’écran contenant différents SSID.

2. Un des réseaux dans le fichier de capture a LaboLAN comme SSID. C’est ce réseau que nous allons étudier dans ce labo. Il est composé seulement de deux stations et d’un AP. Nous allons remplir la tabelle ci-dessous avec les adresses MAC de l’AP et des deux stations (l’adresse de la station STA1 est déjà remplie). Pour trouver l’adresse MAC de l’AP, sélectionnez une des trames beacon de ce réseau (LaboLAN donc), deployez l’entête 802.11 et observez dans les détails de la trame l’adresse TA (Transmitter address). Ne vous sentez pas trop frustrée si vous ne savez pas au début où aller voir dans Wireshark pour trouver cette adresse. Essayez en cliquant dans les différents fenêtres de Wireshark, en posant la question par internet, ou bien en demandant à vos camarades de classe ou au personnel enseignant de vous aider une fois que vous aurez essayé les autres méthodes.

Une fois que vous aurez trouvé la TA, inscrivez-la dans la tabelle. Elle correspond à l’adresse MAC de l’AP puisque les trames beacon sont seulement transmises par l’AP.

Il ne manque que l’adresse de la station STA2. Passez à la page suivante pour des instructions et indices sur comment la trouver.

Tabelle 2. Adresses MAC de l’AP et des deux stations. A remplir par les étudiantes.

|  |  |
| --- | --- |
| Station ou AP | Adresse MAC |
| AP |  |
| STA1 | f0:18:98:14:2a:4a |
| STA2 |  |

Afin de trouver l’adresse MAC de la station STA2, nous utiliserons le fait mentionné précédemment que notre réseau LaboLAN consiste seulement de l’AP et des stations STA1 et STA2. Regardez à nouveau le réseau graphiquement :



Clairement, les trames destinées à l’AP ne peuvent venir que de la station STA1 ou de la station STA2. Si nous utilisons un filtre Wireshark pour n’afficher que ces trames-là, nous devrions obtenir une liste de trames dont certaines viendraient de la station STA1 et les autres de la station STA2. Déployant dans Wireshark l’entête MAC 802.11 des trames affichées et observant la TA de ces trames, nous trouverons l’adresse de la station STA2 (celle qui est différente de l’adresse déjà inscrite dans la tabelle 2).

## Partie 2

## Filtres Wireshark avancés

Les réseaux sans fil 802.11 peuvent être très « bavards ». Nous allons créer des filtres dans la suite de ce laboratoire pour afficher seulement les trames qui nous intéressent, rendant l’analyse plus gérable.

**Pour les prochaines questions, utilisez les adresses MAC de la tabelle 2 que vous venez de remplir.**

3. Donner le filtre pour ne voir que les trames dont les données sont destinées à la station STA2.

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

Attention : afin de déterminer si vous devez créer un filtre en utilisant l’adresse RA, DA, SA ou TA regardez bien les définitions à la tabelle 1.

………………………………………..……………………………………………………….

4. Donner le filtre pour ne voir que les trames reçues par la station STA2. Encore une fois, afin de déterminer si vous devez créer un filtre en utilisant l’adresse RA, TA, SA ou DA, regardez bien les définitions à la tabelle 1.

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

…………………………………………………………………………………………………………

5. Donner le filtre pour ne voir que les trames dont l’expéditeur des données y contenues est la station STA1. Voir les définitions des adresses à la tabelle 1 ci-dessus.

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

…………………………………………………………………………………………………………

6. Créez un filtre qui permette d’afficher toutes les trames transmises par l’AP.

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

…………………………………………………………………………………………………………

7. Voit-on des trames ACK dans la capture précédente ? Sinon, pourquoi ? Indice : Pensez aux adresses qui apparaissent dans l’entête des trams ACK.

…………………………………………………………………………………………………………

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

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

…………………………………………………………………………………………………………

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

Appliquez le filtre et ajoutez une capture d’écran montrant le résultat.

…………………………………………………………………………………………………………

 10. Il est possible de créer des filtres qui utilisent des opérateurs logiques « and » ou « or » dans Wireshark. 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. Pour afficher les trames de données, vous pouvez utiliser un filtre qui utilise le type et le subtype.

…………………………………………………………………………………………………………

## Partie 3

## Captures

## CSMA/CA unicast d’une STA à une autre sans fragmentation

11. Cette question que nous avons résolue en classe sera posée au TE. Dessinez la séquence de trames qui correspond à une transmission unicast d’une station STA1 à une station STA2 utilisant la méthode CSMA/CA sans fragmentation dans un réseau basé sur infrastructure.



Dans le fichier de capture Wireshark que vous avez ouvert avec Wireshark, cherchez une séquence qui corresponde à une transmission unicast comme celle que vous avez dessinée. Voici quelques consignes qui peuvent vous aider à trouver ces séquences :

12. Collez une capture d’écran et donnez les informations suivantes sur les trames :

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

## RTS/CTS unicast (toujours dans un réseau basé sur infrastructure) d’une STA à une autre. Attention : seules les trames transmises par l’AP utilisent RTS/CTS.

 13. Cette question que nous avons résolue en classe sera posée au TE. 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.

14. 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) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## CSMA/CA broadcast depuis une STA dans un BSS

 15. Cette question que nous avons résolue en classe sera posée au TE. Dessinez la séquence de trames qui correspond à une transmission broadcast dans un BSS 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.

16. Collez une capture 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) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Retransmissions

 17. 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. Le bit qui identifie ces trames s’appelle retry.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Techniques pour la recherche des séquences de trames

*Coloriage :*

Les captures Wireshark de trames ont souvent des milliers, voire de dizaines de milliers de trames. Afin de chercher des types spécifiques de trames, vous avez déjà utilisé des filtres.

Si en plus de chercher des trames vous avez besoin de trouver des séquences de trames, l’utilisation de filtres d’affichage peut être combinée avec une fonctionnalité de Wireshark qui permet d’afficher en différentes couleurs les trames qui résulterait de l’application de filtres.

Afin d’afficher des trames en une couleur de votre choix, cliquer d’abord sur View dans le menu de Wireshark, puis sur Coloring Rules…

Une nouvelle fenêtre s’ouvrira qui vous permettra de ajouter des filtres et de définir le coloriage des trames résultantes de ces filtres.

Un exemple serait la recherche des séquences correspondant à une séquence CSMA/CA dans un réseau basé sur infrastructure. Comme vous le savez, la séquence contient les 4 trames suivantes :

1. Trame de données de la station STA1 vers l’AP
2. Trame ACK de l’AP vers la station STA1
3. Trame de données de l’AP vers la station STA2
4. Trame ACK de la station STA2 vers l’AP

Si dans les Coloring Rules … nous faisons en sorte que les trames de données transmises par la station STA1 vers l’AP soient colorées en vert, les trames de données transmises par l’AP vers la station STA2 soient colorées en bleu et les trames ACK soient colorés en jaune, nous pourrions observer visuellement les séquences

Trame de données de la station STA1 vers l’AP

Trame ACK de l’AP vers la station STA1

Trame de données de l’AP vers la station STA2

Trame ACK de la station STA2 vers l’AP

*Filtres :*

Le type de trames 802.11 est défini par deux champs dans l’entête : le type et le subtype.

Il y a trois types de trames :

* Les trames de données qui, sans surprise, sont des trames qui transportent des données,
* Les trames de contrôle, comme les trames ACK, RTS et CTS qui ne transportent pas de données mais qui sont nécessaires au bon déroulement des protocoles tells CSMA/CA et RTS/CTS
* Les trame de gestion qui sont utilisées pour l’établissement, la libération et la gestion du réseau. Un exemple d’une trame de gestion est la trame beacon.

On peut se baser sur le type et le subtype pour créer des filtres. Par exemple, pour n’afficher que des ACK, le filtre suivant peut être utilisé :

wlan.fc.type\_subtype == 0x001d

De la même façon, on peut trouver des filtres pour les trames de données et de gestion.