Pascal Cotret
ENSTA Bretagne

Introduction aux réseaux
FIPA 2024 - Examen

28 octobre 2022

Table des matières

Quelques consignes 2
1. Exercice - Analyse de trames réseaux 2
2. Wifi 4
2.1. Rappels sur le fonctionnement du Wifi 4
2.2. Exercice 8
3. Analyse des trames d'un réseau local Ethernet 9
4. Exercice bonus - Forensique des réseaux 11

N'ayez pas peur de la longueur du document, la partie Wifi contient des rappels de cours sur 4-5 pages.

Quelques consignes

- Durée : 2h. Tout dépassement sera sanctionné.
- Format libre : LibreOffice, Word, Markdown, PDF. Je prends tout
- Bien que les réponses soient souvent courtes, la rédaction sera prise en compte dans la notation finale (par exemple, l'orthographe).
- A la fin des 2 heures, le document est à rendre sur Moodle dans le dépôt prévu à cet effet. Si et seulement si problème, vous pouvez envoyer par mail : pascal.cotret@ensta-bretagne.fr

L'exercice bonus est, comme son nom l'indique, bonus. Je calcule une note sur 20 sur les 3 premiers exercices. Si **et seulement si** vous avez fini avant, vous pouvez regarder l'exercice 4.

1. Exercice - Analyse de trames réseaux

On suppose qu'un ordinateur A est relié à Internet selon la topologie illustrée par la figure 1.1. Cet ordinateur est relié à un réseau local via un commutateur Ethernet (S). D'autre machines sont présentes sur ce réseau et fournissent différents services réseaux (S1 à S3). Ce réseau local est également relié à Internet via un routeur (R).

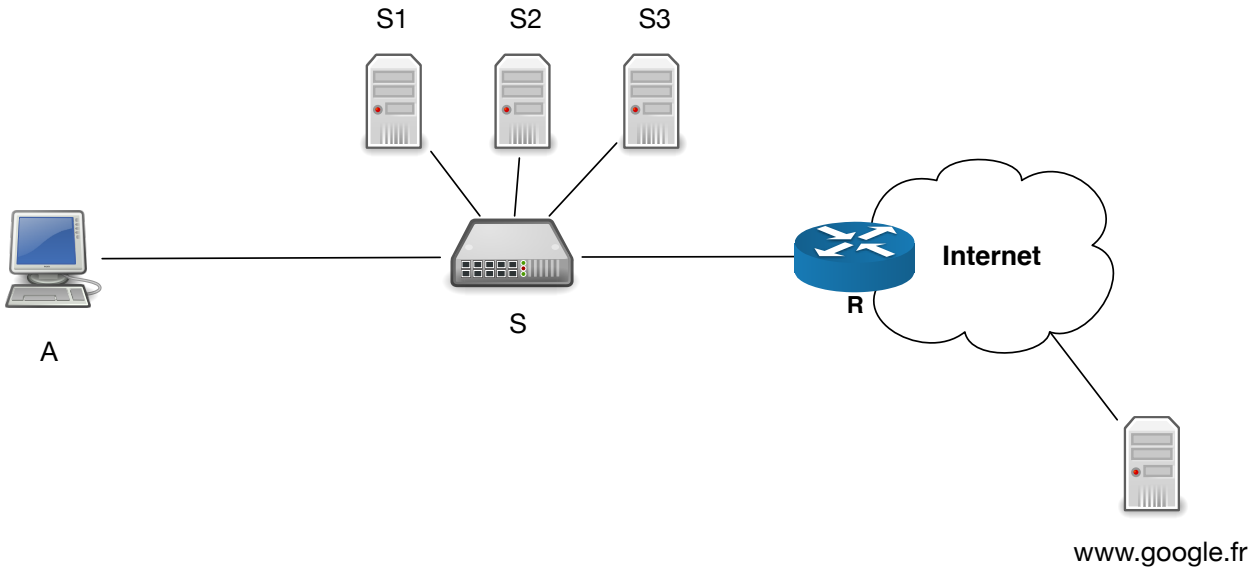


FIGURE 1.1. – Architecture du réseau

On réalise une capture réseau sur l'ordinateur lorsque l'utilisateur navigue sur le site `www.google.fr`. La capture est illustrée par la figure 1.2 (attention, la colonne "destination" est avant la colonne "source").

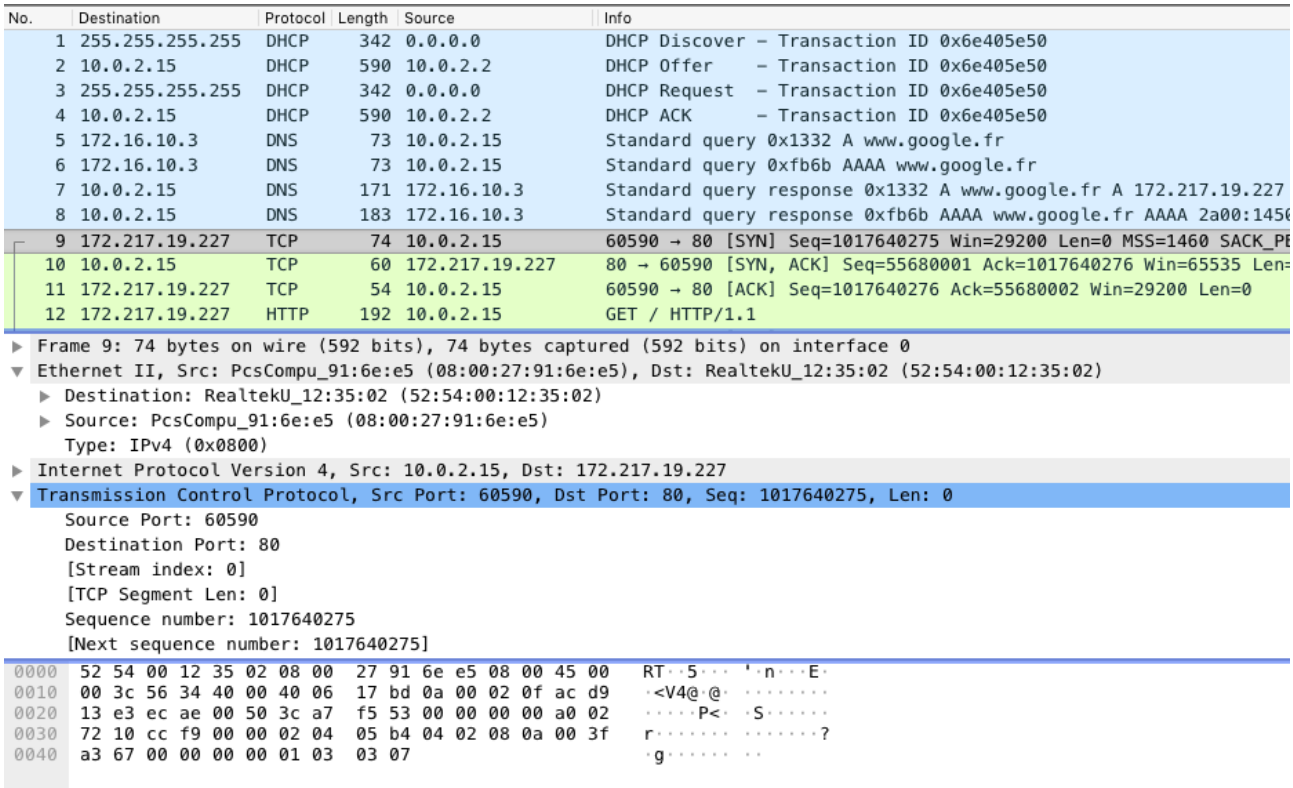


FIGURE 1.2. – Trace réseau capturée sur A

Question 1. Quelle est l'adresse IP de la machine A ?

Question 2. D'après la trace réseau, comment la machine A a-t-elle obtenu cette adresse IP ?

Question 3. À quoi correspond l'adresse IP 255.255.255.255 ? Pourquoi est-elle utilisée dans cette trace réseau ?

Question 4. L'adresse MAC `52:54:00:12:35:02` est elle l'adresse de la machine A, du commutateur S, du routeur R ou du serveur de Google ? Pourquoi ?

Question 5. Quelle est l'adresse IP du serveur de Google dans la trace ?

Question 6. Comment la machine A a-t-elle pu obtenir cette adresse IP ?

2. Wifi

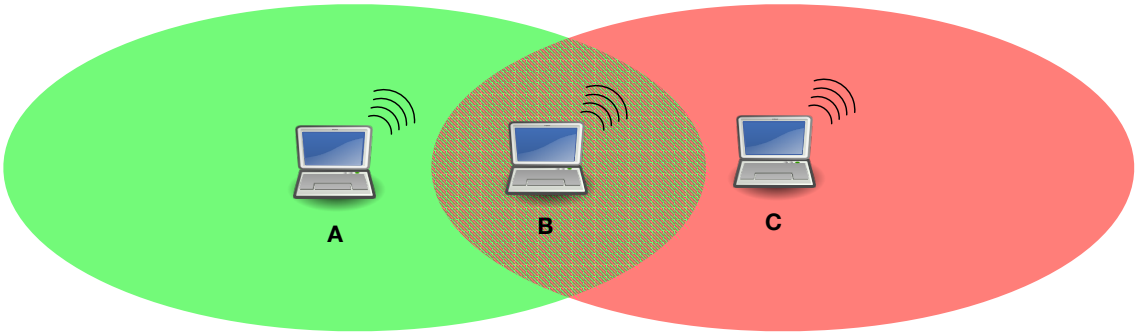
2.1. Rappels sur le fonctionnement du Wifi

Les réseaux sans fil comme les réseaux Wifi doivent faire face à des contraintes spécifiques :

- La portée radio peut varier fortement : la puissance du signal décroît en fonction de la distance et des types de matériaux parcourus ;
- Des interférences peuvent perturber le signal : en effet, les bandes de fréquences allouées sont souvent utilisées par d'autres sources (micro-ondes, autres communications radio, etc.) ;
- Les réflexions multiples perturbent la réception du signal : le signal réfléchi arrive à destination avec différents temps de retard.

Ces contraintes influencent les techniques d'accès au support de communication utilisées par ces réseaux. Par exemple, le problème des « stations cachées » exclut d'utiliser les techniques de détection de collision comme CSMA/CD, utilisée dans Ethernet. Ce problème est illustré par la figure 2.3 : la station A est à portée radio de B, B est à portée radio de C mais en revanche A et C sont hors de portée l'une de l'autre. Ainsi, si A communique avec B et que simultanément C communique avec B, ni A ni C ne peuvent détecter la collision.

FIGURE 2.3. – Problème de la station cachée



La norme 802.11 utilise donc une autre technique d'accès au support appelée CSMA/CA (pour *Collision Avoidance*). Avant d'émettre, une station écoute pendant un certain temps (appelé SIFS) pour s'assurer que le support est libre. Cela permet de limiter les collisions : si une deuxième station veut émettre et qu'elle est à portée radio de la première, elle diffère l'émission de son message, comme l'illustre la figure 2.4. Comme le récepteur est le seul à pouvoir détecter une éventuelle collision, il acquitte chacun des messages qui lui ont été correctement transmis. Pour cela, il vérifie le CRC de chaque message reçu. En cas de collision, la vérification échoue et la station n'envoie pas d'acquittement, comme l'illustre la figure 2.5. Les stations émettrices détectent au bout d'un certain temps l'absence d'acquittement. Elles tentent alors de renvoyer leurs paquets après un temps aléatoire (*backhoff time*). Ce temps aléatoire évite de générer une nouvelle collision.

FIGURE 2.4. – CSMA/CA

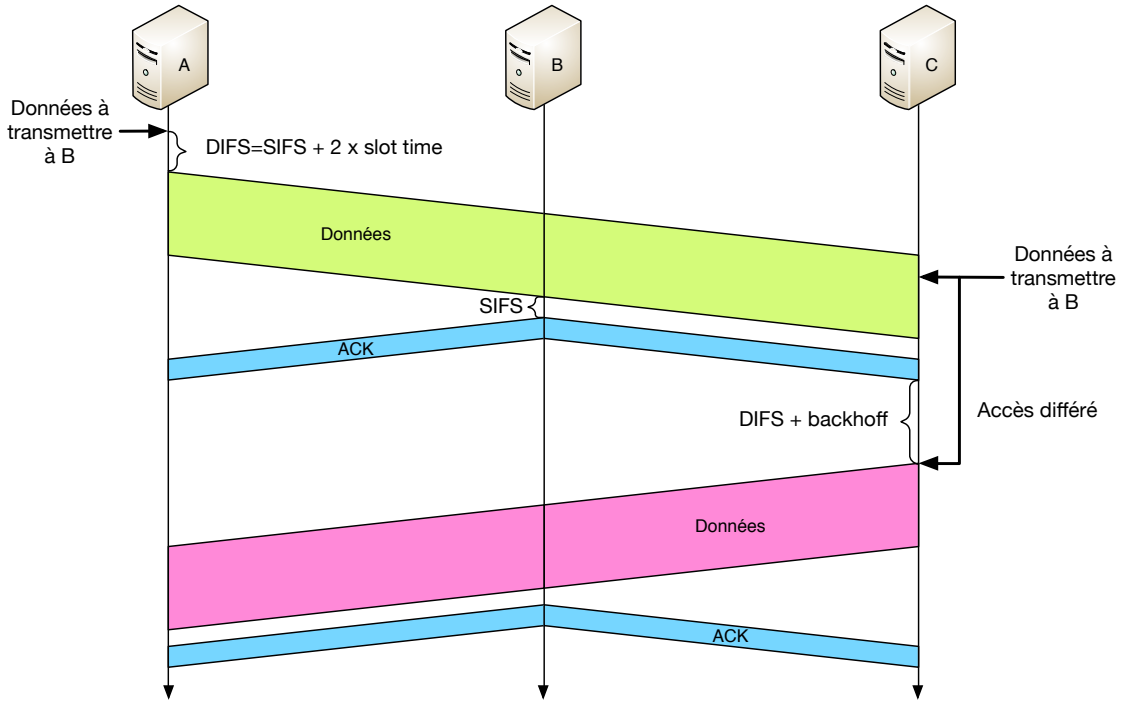
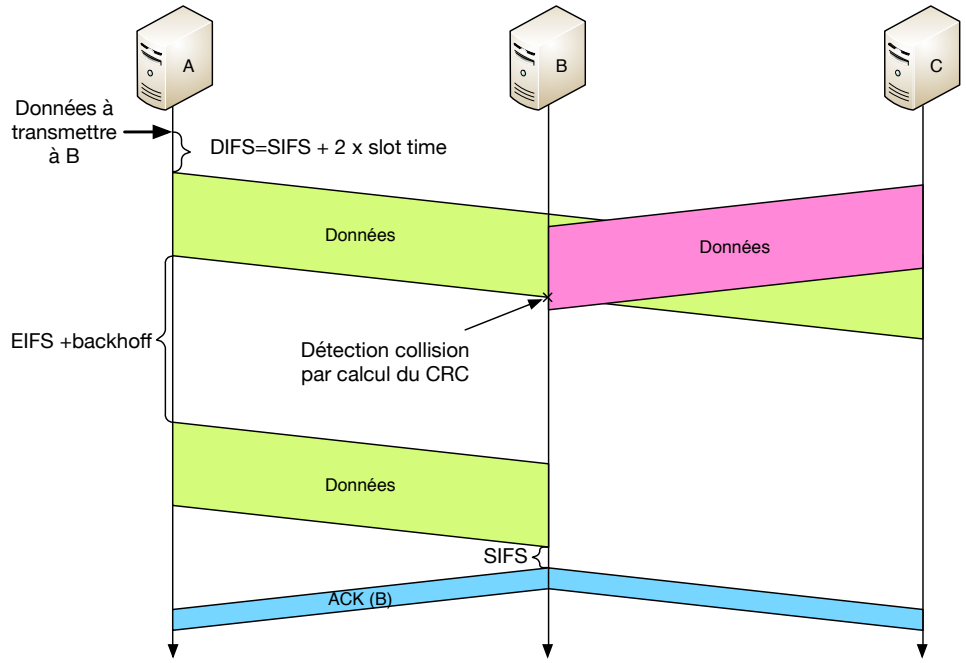


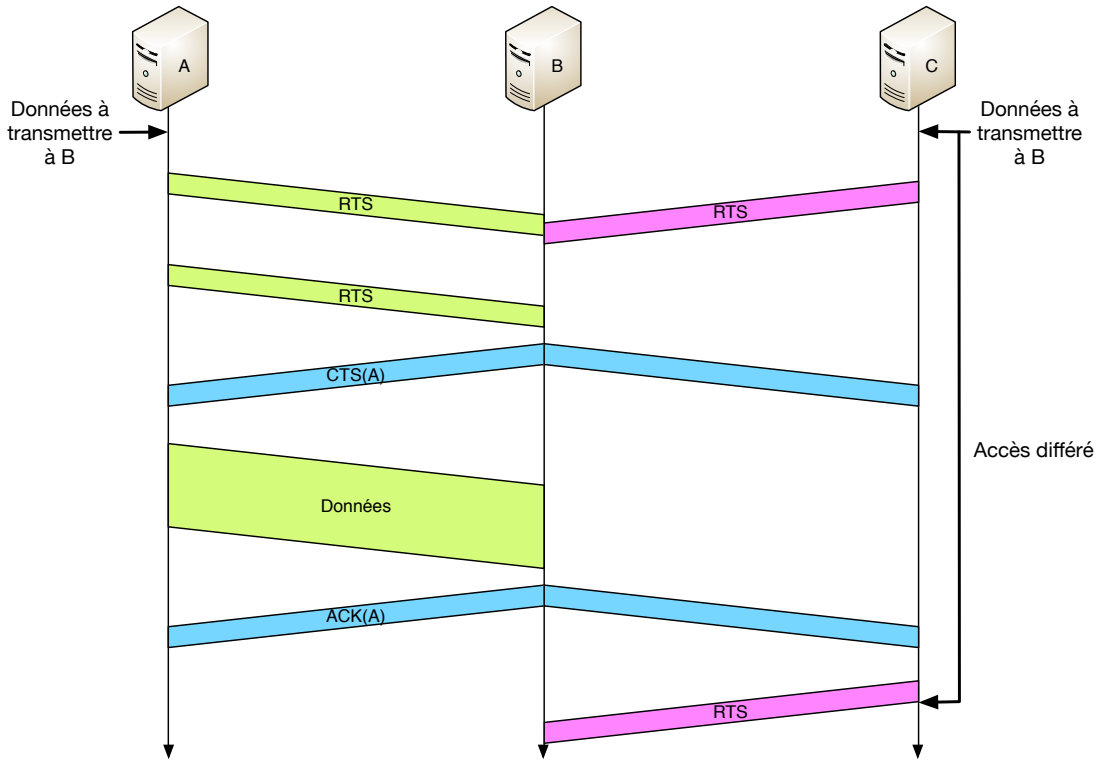
FIGURE 2.5. – CSMA/CA : détection de collision



En cas de détection de collision, l'émetteur doit renvoyer l'ensemble de la trame, ce qui induit une perte de temps et donc de débit. Pour limiter ce phénomène, les stations peuvent utiliser un mécanisme additionnel de réservation de « temps de parole ». La station qui souhaite émettre envoie d'abord une trame RTS (*Ready To Send*). Dans cette trame, la station annonce un slot de temps qu'elle souhaite réserver pour pouvoir émettre sa trame. La station réceptrice confirme la réservation par une trame CTS (*Clear To Send*) qu'elle envoie à toutes les stations à portée radio. La station qui a envoyé la trame RTS peut alors commencer d'envoyer les données qu'elle souhaitait émettre. Les autres stations diffèrent systématiquement leurs éventuels envois de données pour éviter les collisions.

Avec cette approche, seule la trame RTS peut faire l'objet d'une collision, comme l'illustre la figure 2.6. Mais puisqu'il s'agit d'une trame de longueur très réduite, cela limite le temps perdu. Toutefois, le gain n'est significatif que pour les transmissions de paquets de grande taille. En pratique, ce mécanisme n'est pas toujours utilisé, notamment lors de l'émission de paquets ne contenant que des acquittements TCP.

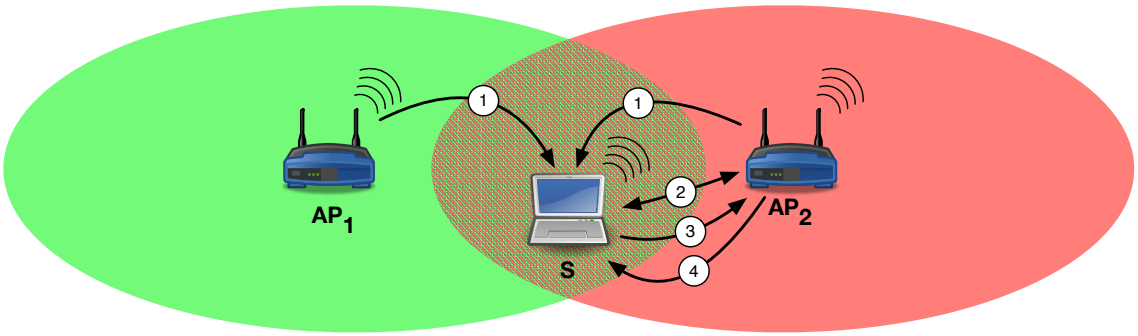
FIGURE 2.6. – RTS/CTS



Il existe différentes architectures de réseaux Wifi. Toutefois, les plus courantes utilisent le mode *infrastructure*. Dans ce mode, les communications entres les différentes stations passent systématiquement par un nœud central : le point d'accès (*Access Point*). Avant de pouvoir communiquer avec les autres stations d'un tel réseau, une station doit d'abord s'authentifier et s'associer avec le point d'accès. Pour cela, la station doit sélectionner le réseau qu'elle souhaite rejoindre en spécifiant son SSID. Les différents échanges se déroulent dans l'ordre suivant, illustré par la figure 2.7 :

1. Les points d'accès émettent régulièrement des trames balises (*beacon frames*) en *broadcast*. Ces trames annoncent les SSID des réseaux gérés par le point d'accès, les fonctionnalités supportées, etc.
2. La station s'authentifie auprès du point d'accès en échangeant avec lui des trames de type *authentication*.
3. La station émet ensuite une demande d'association (*association reQuestion*)
4. Le point d'accès confirme par une trame *association response*

FIGURE 2.7. – Association



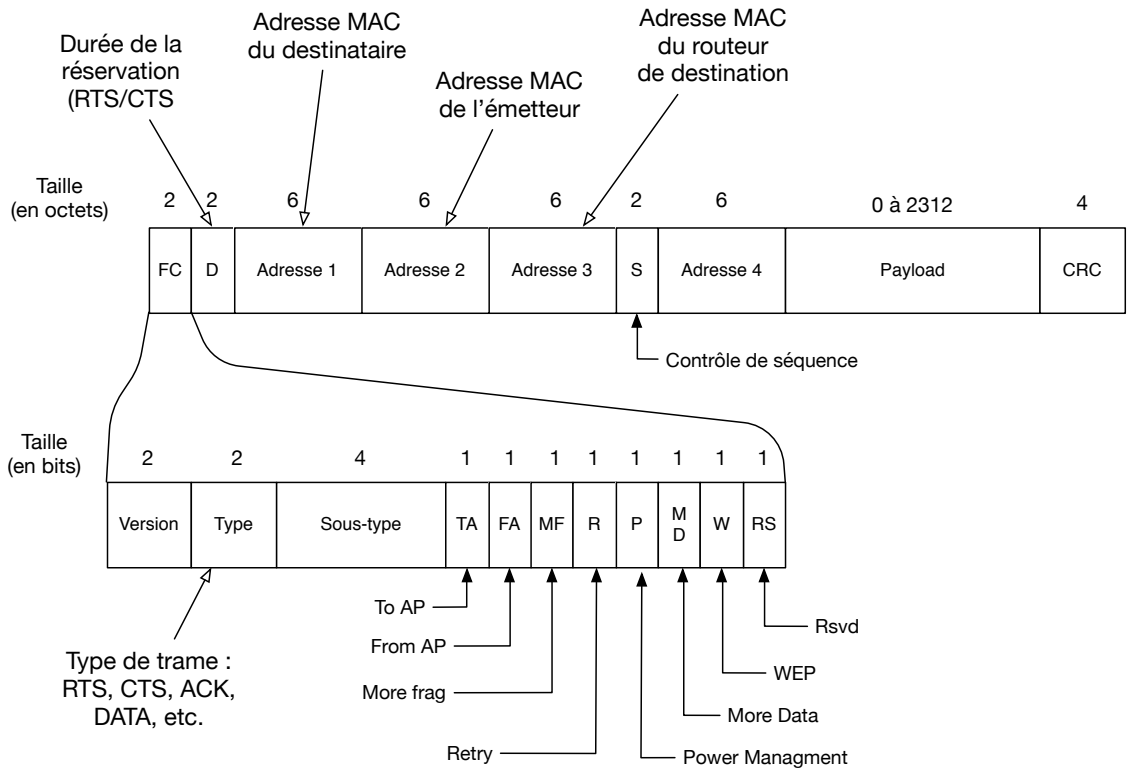
Les trames 802.11, illustrées par la figure 2.8 sont plus complexes que les trames Ethernet, en raison notamment des différents types de messages de gestion utilisés par le protocole. On remarque notamment qu'elles utilisent trois adresses MAC :

— la première désigne le destinataire au sein du réseau Wifi ;
— la seconde désigne l'émetteur au sein du réseau Wifi ;
— la dernière désigne l'adresse du routeur auquel est relié le point d'accès.

Les différents types de trames sont désignés par les champs `Type` et `Sous-type`. Les valeurs des principaux types et sous-types, ainsi que les filtres Wireshark correspondants, sont décrits sur ce site Web de Cisco :

https://community.cisco.com/t5/wireless-mobility-documents/802-11-frames-a-starter-guide-to-learn-wireless-sniffer-traces/ta-p/3110019

FIGURE 2.8. – Format trame 802.11



2.2. Exercice

Pour cet exercice, vous utiliserez le fichier `802_11.pcap`. Ce fichier correspond à une capture effectuée par l'un des auteurs de l'ouvrage « Computer Networking : A Top-Down Approach ».

Question 7. Quels sont les différents points d'accès que vous pouvez identifier ? Quels sont les SSID des réseaux qu'ils annoncent ?

Question 8. Quelle est l'adresse MAC de destination des *beacon frames* ?

Question 9. Quel est l'intervalle d'émission de ces *beacon frames* ?

Question 10. Quels sont les débits supportés par le point d'accès *30 Munroe St* ?

Question 11. Le paquet n° 474 correspond à une demande de connexion TCP (SYN) effectuée par une machine déjà associée à l'un des points d'accès. Que désignent les trois addresses MAC de cette trame ? À quelles interfaces réseau correspondent-elles ?

Question 12. Quelles sont les adresses IP source et destination de cette trame ? A quels nœuds du réseau correspondent ces adresses ?

Question 13. Ce paquet a-t-il bien été reçu par le point d'accès ?

Question 14. Identifiez les demandes d'authentification. Vous pouvez pour cela utiliser le filtre d'affichage de Wireshark `wlan.fc.type_subtype == 0x000b`. Sur quel point d'accès la machine `00:13:02:d1:b6:4f` tente-t-elle d'abord de s'authentifier ? Quel type d'authentification tente-t-elle de réaliser ? Est-ce que le point d'accès lui répond ?

Question 15. Sur quel autre point d'accès la machine tente-t-elle ensuite de s'authentifier ? Quelle est la réponse de ce point d'accès ?

Question 16. Quelles sont les trames d'association correspondant à cette dernière authentification ? Quels sont les débits supportés par la machine ? Quels sont ceux supportés par le point d'accès ?

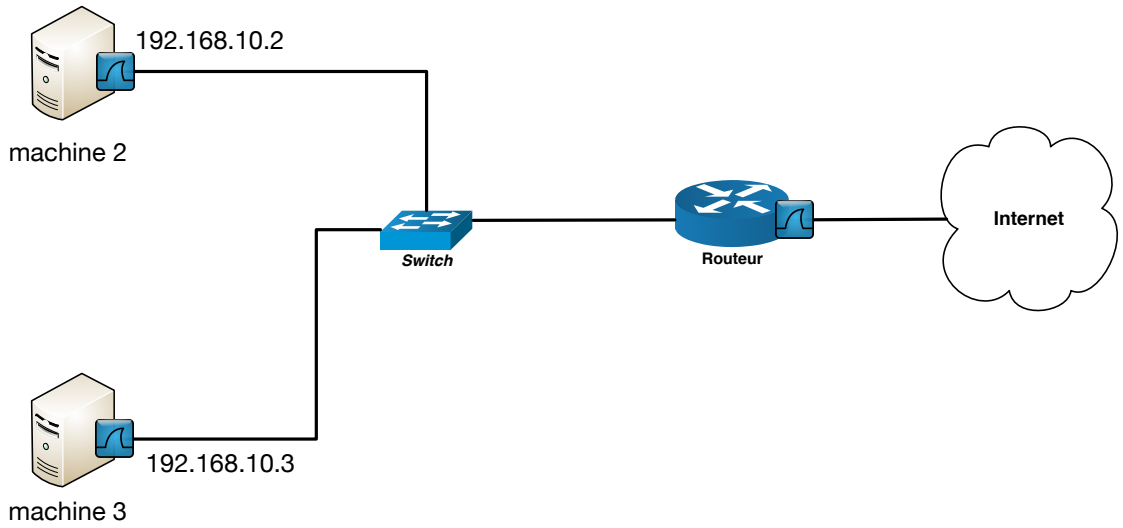
Question 17. À quoi correspond le message n° 2152 ? Quels sont les noeuds qui répondent à ce message ? Quelle est leur réponse ?

3. Analyse des trames d'un réseau local Ethernet

i Il s'agit d'un exercice qui fait suite à un exercice du TD noté. Les éléments de contexte sont donc remis dans ce sujet. Pour autant, les questions sont indépendantes : vous devriez pouvoir les résoudre sans regarder le sujet du TD.

On considère le réseau illustré par la figure 3.9.

FIGURE 3.9. – Plan du réseau



Le logiciel Wireshark a été utilisé pour capturer le trafic à trois endroits distincts de ce réseau (matérialisés par les icônes Wireshark) : sur l'interface réseau de la machine 2, sur l'interface réseau de la machine 3 et sur l'interface du routeur qui le relie à Internet.

L'exercice est basé sur une analyse du fichier `machine3.pcapng`.

On vous demande par la suite d'analyser le trafic contenu dans ces fichiers à l'aide de Wireshark afin de répondre aux différentes questions.

Question 18. En observant les paquets 71 à 74, quel est le protocole de transport utilisé pour échanger ces différents messages ? Quelles sont les garanties offertes par ce protocole ?

Question 19. Comment le destinataire du paquet n°78 peut-il identifier le protocole de transport utilisé ? Comment peut-il identifier le protocole applicatif ?

Question 20. Quels sont les paquets qui établissent la connexion ? Ceux qui la terminent ? Expliquer le principe d'ouverture et de fermeture de connexion.

Question 21. À quoi sert le paquet n°79 ?

Question 22. Quels sont les ports source et destination des paquets n°78 et n°79 ? Pourquoi sont-ils inversés ? Comment ont-il été choisis par le client et le serveur ?

Question 23. Quelle est l'adresse IP du routeur ?

Question 24. Ouvrez maintenant le fichier `routeur.pcapng`. Quels sont les numéros des paquets qui correspondent aux messages évoqués dans les questions précédentes ? Est-ce que ces paquets sont identiques aux précédents (ont-il les mêmes adresses IP et MAC, source et destination ?) Pourquoi ?

Question 25. À partir des messages de la trace, peut-on déterminer l'adresse MAC du serveur de Google ? Pourquoi ?

4. Exercice bonus - Forensique des réseaux

Question 26. Ouvrez le fichier `telnet.pcap`.
- Quel utilisateur s'est logué sur la machine 192.168.0.1 ?
- Qu'est-ce que l'utilisateur a fait ensuite ?

Question 27. Ouvrez le fichier `chat.dmp`.
- Quel type de protocole est utilisé ?
- Quelles sont les adresses mails des deux interlocuteurs ?
- Que disent-ils à propos de l'administrateur système ?