TD1

WiFi – Authentification et Association

Exercice 1 - Fonctionnement du WiFi - Généralités

Q. 1.1 : Conseilleriez-vous d'utiliser le même canal de fréquence pour les différents points d'accès ou d'en choisir un différent pour chacun ? Pourquoi ?

Je ne conseillerais pas d'utiliser le même canal de fréquence pour les différents points d'accès, car cela pourrait entraîner des interférences entre les réseaux. C'est mieux de choisir des canaux différents pour éviter des interférences et optimiser les performances du réseau.

Q. 1.2 : Proposer 4 domaines d'utilisation des réseaux sans fil.

Les réseaux sans fil peuvent être utilisés dans les réseaux en intérieur comme les maisons pour connecter des appareils personnels à Internet sans fil. Ils sont également importants pour les entreprises pour permettre aux employés de se connecter au réseau. Les établissements publics, comme les cafés, les aéroports et les hôtels. Pour finir les réseaux IoT utilisent le WiFi pour connecter des appareils intelligents comme les capteurs et caméras.

IoT : réseau d'objets et de terminaux connectés équipés de capteurs

Q. 1.3 : Quelles caractéristiques vous paraissent importantes lors de la phase de spécification d'un nouveau réseau local sans fil ?

Il faut faire attention à la couverture du réseau pour s'assurer qu'il couvre toute la zone. La sécurité est également importante pour protéger les données contre les accès non autorisés. Le débit du réseau doit être suffisant aussi.

Q. 1.4 : Lister quelques pratiques de sécurité de base en WiFi.

L'utilisation d'un mot de passe fort pour le réseau, activer le chiffrement WPA3, changer régulièrement le mot de passe du réseau. Désactiver la diffusion du SSID permet de rendre le réseau moins visible. C'est important de mettre à jour régulièrement le firmware des points d'accès pour bénéficier des dernières améliorations de sécurité.

Exercice 2 - Association avec Point d'Accès

Q. 2.1 : Quels sont les différents points d'accès que vous pouvez identifier ? Quels sont les SSID des réseaux qu'ils annoncent ?

Les SSID des réseaux annoncés par les points d'accès se trouvent dans les "Tagged parameters" de la couche IEEE 802.11.

Q. 2.2 : Quelle est l'adresse MAC de destination des beacon frames ?

L'adresse MAC de destination des beacon frames est l'adresse de broadcast, qui est `ff:ff:ff:ff:ff:ff`.

Q. 2.3 : Quel est l'intervalle d'émission de ces beacon frames ?

L'intervalle d'émission des beacon frames est de 100 ms.

Q. 2.4 : Quels sont les débits supportés par le point d'accès 30 Munroe St ?

Pour connaître les débits supportés par le point d'accès "30 Munroe St", il faut examiner les "Supported Rates" dans les beacon frames émises par ce point d'accès.

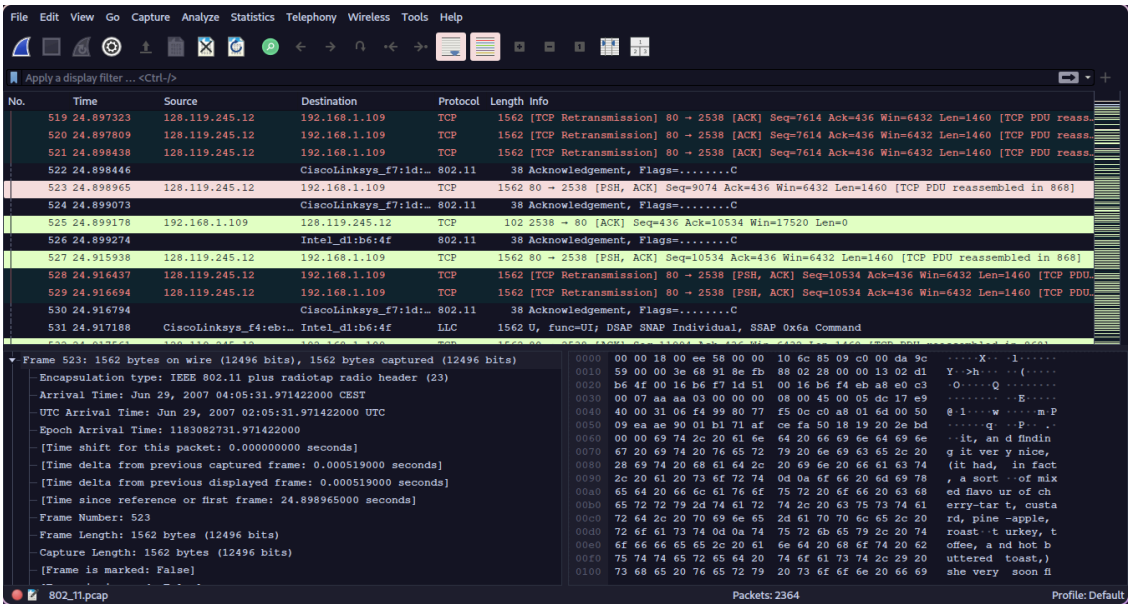
Q. 2.5 : Le paquet n°474 correspond à une demande de connexion TCP (SYN) effectuée par une machine déjà associée à l'un des points d'accès. Que désignent les trois adresses MAC de cette trame ? À quelles interfaces réseau correspondent-elles ?

equête DNS : La machine a envoyé une requête DNS pour résoudre le nom de domaine `gala.cs.umass.edu`.

Réponse DNS : Le serveur DNS a répondu avec l'adresse IP `128.119.245.12`.

Q. 2.6 : Quelles sont les adresses IP source et destination de cette trame ? À quels nœuds du réseau correspondent ces adresses ?

- **Adresse IP source :** `128.119.245.12`
- **Adresse IP destination :** `192.168.1.109`
- **Adresse IP source (`128.119.245.12`)**
- **Adresse IP destination (`192.168.1.109`)**

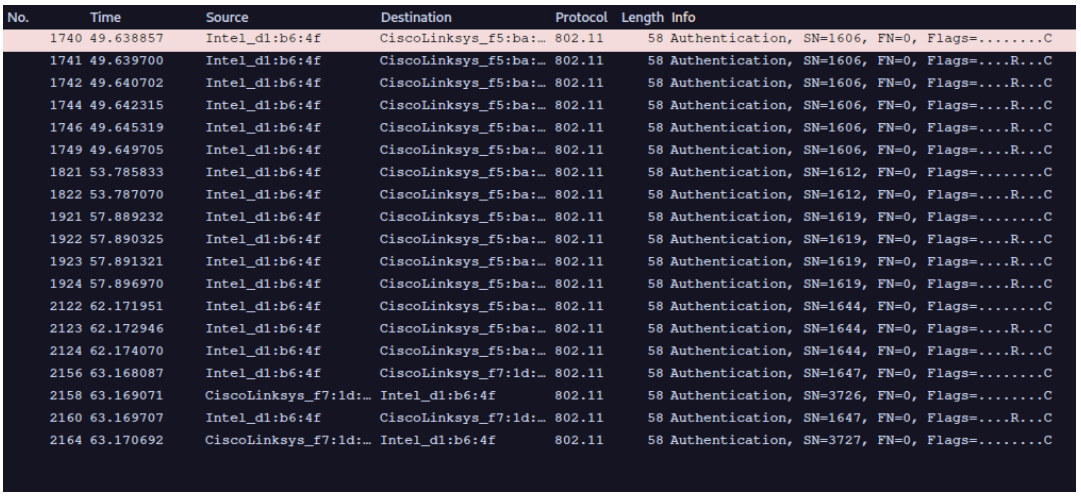


Q. 2.7 : Ce paquet a-t-il bien été reçu par le point d'accès ?

Dans la capture d'écran, la trame n°526 montre un accusé de réception (ACK) envoyé par `192.168.1.109` à `128.119.245.12`. Cela indique que le paquet a bien été reçu par la station de destination.

Q. 2.8 : 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 ?

La machine `00:13:02:d1:b6:4f` tente d'abord de s'authentifier sur le point d'accès `CiscLinksys_f5:ba:...` en utilisant une authentification ouverte. Le point d'accès répond à cette demande, comme le montrent les trames d'authentification



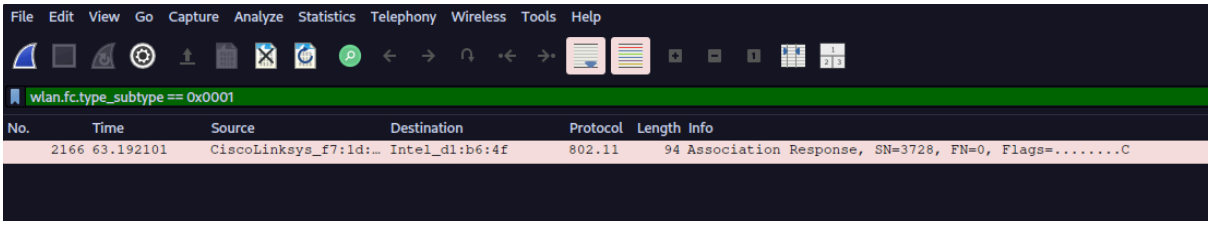
No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	Intel_d1:b6:4f	CiscoLinksys_f5:ba:…	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	Intel_d1:b6:4f	CiscoLinksys_f7:1d:…	802.11	58	Authentication, SN=1647, FN=0, Flags=........C
2158	63.169071	CiscoLinksys_f7:1d:…	Intel_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C
2160	63.169707	Intel_d1:b6:4f	CiscoLinksys_f7:1d:…	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	CiscoLinksys_f7:1d:…	Intel_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=........C

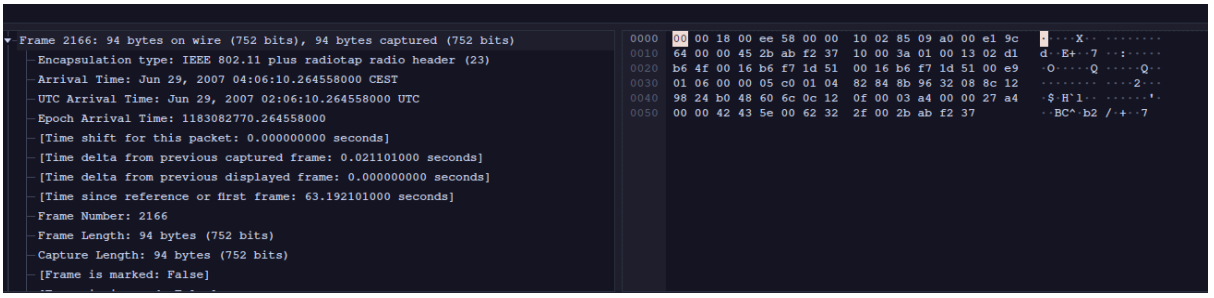
Q. 2.9 : Sur quel autre point d'accès la machine tente-t-elle ensuite de s'authentifier ? Quelle est la réponse de ce point d'accès ?

La machine tente ensuite de s'authentifier sur le point d'accès “`LinksysGroup_67:22`”.

Q. 2.10 : 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 ?

- **Trames d'association :** La trame n°2166 est une "Association Response" correspondant à la dernière authentification.
- **Débits supportés :** 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, et 54 Mbps.





Q. 2.11 : À quoi correspond le message n°2152 ? Quels sont les nœuds qui répondent à ce message ? Quelle est leur réponse ?

Le message n°2152 est une trame de "Probe Request" envoyée par la station pour découvrir les points d'accès disponibles. Les points d'accès répondent avec des trames de "Probe Response", indiquant leur présence et leurs capacités.