

Teaching-HEIGVD-SRX-2020-Laboratoire-WiFi

Vous aurez besoin de `wireshark` et du logiciel `aircrack-ng` pour ce laboratoire.

Si vous utilisez une distribution Kali, tout est déjà pré-installé. Pour la version Windows du logiciel `aircrack-ng` ou pour son installation sur d'autres distributions, référez-vous au [site web aircrack-ng](http://site.web.aircrack-ng) et/ou au gestionnaire de paquets de votre distribution.

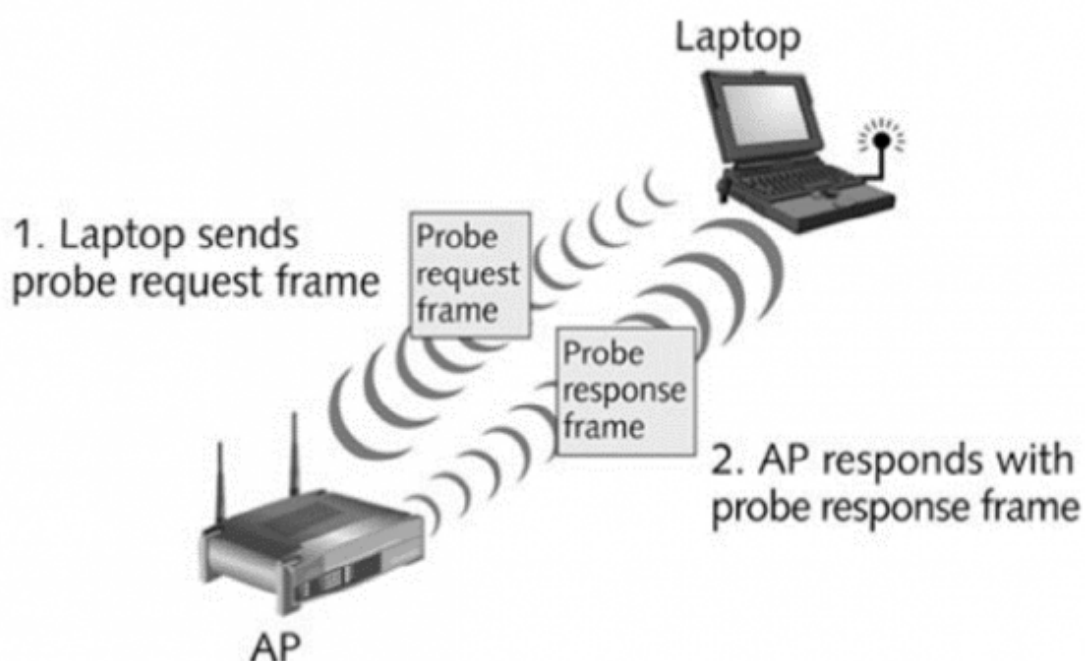
Identification d'un dispositif

Introduction

L'objectif de cette partie est de vous familiariser avec les captures provenant de l'interception de données sans fils et de comprendre quels types d'informations utiles peuvent être obtenues à partir des dites captures.

Comme vous l'avez étudié dans le cours théorique, l'environnement le plus adapté et riche pour capturer et analyser/exploiter les données des réseaux sans-fils est Linux. Pourtant, une machine Windows peut être utilisée avec `wireshark` pour analyser du trafic déjà capturé par d'autres moyens. L'outil le plus utilisé pour le craquage de réseaux sans fils, la suite `aircrack`, est aussi disponible sur Windows. Malgré les limitations imposées par la carence de drivers en mode monitor pour Windows pour capturer le trafic nécessaire, `aircrack` peut être utilisé pour analyser des captures faites par d'autres moyens et obtenir les clés WEP ou les passphrases WPA.

L'une des informations de plus intéressantes et utiles que l'on peut obtenir à partir d'un client sans fils de manière entièrement passive (et en clair) se trouve dans la trame `Probe Request` :



Dans ce type de trame, utilisée par les clients pour la recherche active de réseaux, on peut retrouver :

- L'adresse physique (MAC) du client (sauf pour dispositifs iOS 8 ou plus récents et les versions les plus récentes d'Android...).
 - Utilisant l'adresse physique, on peut faire une hypothèse sur le constructeur du dispositif sans fils utilisé par la cible.
 - Elle peut aussi être utilisée pour identifier la présence de ce même dispositif à des différents endroits géographiques où l'on fait des captures, même si le client ne se connecte pas à un réseau sans fils.
- Des noms de réseaux (SSID) recherchés par le client.
 - Un Probe Request peut être utilisé pour « tracer » les pas d'un client. Si une trame Probe Request annonce le nom du réseau d'un hôtel en particulier, par exemple, ceci est une bonne indication que le client s'est déjà connecté au dit réseau.
 - Un Probe Request peut être utilisé pour proposer un réseau « evil twin » à la cible.

Travail à réaliser

Nous allons utiliser une capture Wireshark pour essayer de déterminer si une cible se trouvait présente à l'HEIG-VD, lieu où une capture devant être analysée, a été faite.

Nous savons que la cible s'est hébergée à l'hôtel « Black Rain » et qu'elle a aussi visité un Starbucks où elle s'est peut-être servie du Wi-Fi gratuit.

Exercice :

- Copier [le fichier de capture](#) sur votre machine locale
- Ouvrir le fichier avec Wireshark
- Analyser la capture pour déterminer l'adresse MAC du dispositif de la cible
- Utiliser un filtre d'affichage Wireshark pour montrer uniquement les trames du type **Probe Request**
- Répondre aux questions suivantes :

Question : Quel filtre avez-vous utilisé

Réponse : Nous avons utilisé le filtre : wlan.fc.type_subtype == 0x0004 qui permet d'afficher les Probe Request

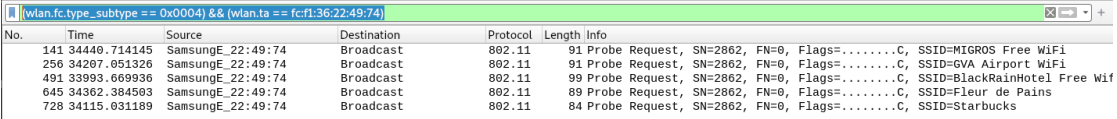
Question : Quel est l'adresse MAC de la cible ?

Réponse : fc:f1:36:22:49:74

On cherche les probe request pour starbucks, seulement 1 a starbucks dans ses informations

Question : Quel est le nom du constructeur de l'interface sans fils de la cible ?

Réponse : Samsung comme indiqué sous la colonne "Source"



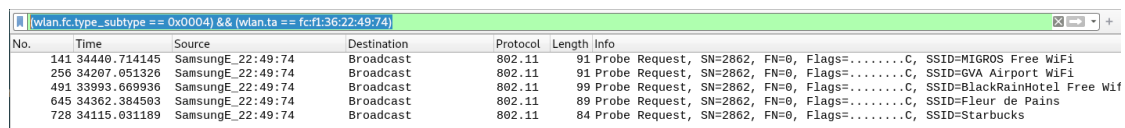
No.	Time	Source	Destination	Protocol	Length	Info
141	34440.714145	SamsungE_22:49:74	Broadcast	802.11	91	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=MIGROS Free WiFi
256	34207.051326	SamsungE_22:49:74	Broadcast	802.11	91	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=GVA Airport WiFi
491	33993.669936	SamsungE_22:49:74	Broadcast	802.11	99	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=BlackRainHotel Free Wif
645	34362.384593	SamsungE_22:49:74	Broadcast	802.11	89	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=Fleur de Pains
728	34115.031189	SamsungE_22:49:74	Broadcast	802.11	84	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=Starbucks

Question : Quel autres endroits la cible a-t-elle probablement visités ?

Réponse : Migros, GVA Airport, Black Rain, Fleur de Pains, Starbucks

On cherche les autres probes avec cette adresse mac:

```
wlan.fc.type_subtype == 0x0004 && wlan.ta == fc:f1:36:22:49:74
```



No.	Time	Source	Destination	Protocol	Length	Info
141	34440.714145	SamsungE_22:49:74	Broadcast	802.11	91	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=MIGROS Free WiFi
256	34207.051326	SamsungE_22:49:74	Broadcast	802.11	91	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=GVA Airport WiFi
491	33993.669936	SamsungE_22:49:74	Broadcast	802.11	99	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=BlackRainHotel Free Wif
645	34362.384503	SamsungE_22:49:74	Broadcast	802.11	89	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=Fleur de Pains
728	34115.031189	SamsungE_22:49:74	Broadcast	802.11	84	Probe Request, SN=2862, FN=0, Flags=.....C, SSID=Starbucks

Réseaux protégés par WEP

Introduction

La norme originale 802.11 spécifie WEP comme étant une méthode pour gérer l'accès au réseau (authentification) et pour la confidentialité de données (chiffrement).

Bien que trouvée faible et exploitée depuis de nombreuses années, cette méthode continue à être utilisée dans beaucoup de pays. Elle est toujours très répandue dans plusieurs zones du tiers monde, mais on retrouve avec étonnement des réseaux WEP aux USA et dans des pays de l'Europe et l'Asie.

Travail à réaliser

Nous allons nous servir de l'outil `aircrack-ng` pour retrouver la clé de chiffrement WEP utilisée pour protéger un réseau dont nous avons une capture avec assez de trafic pour cracker la clé. Une fois la clé récupérée, nous l'utiliserons Wireshark pour rendre la capture lisible.

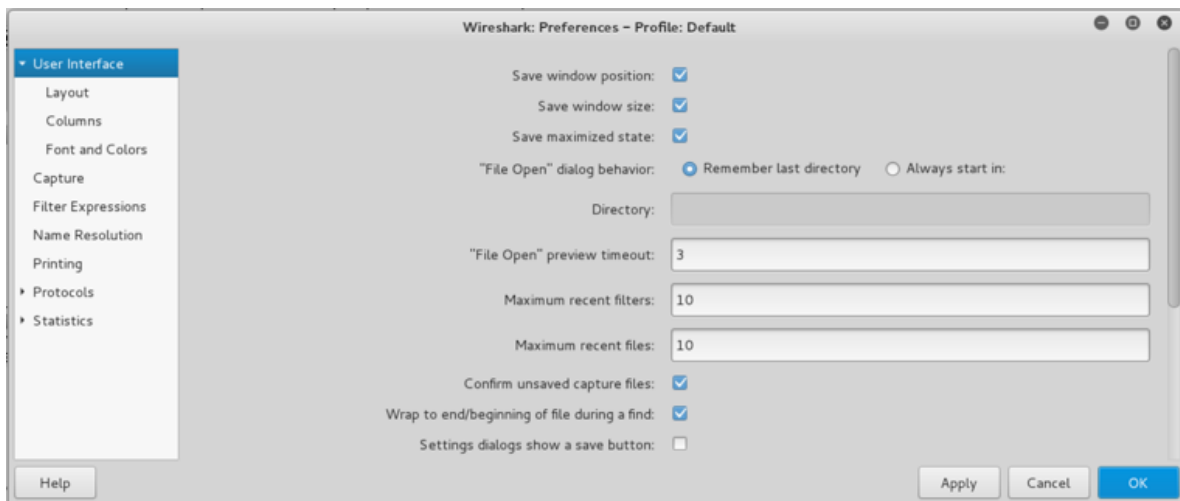
Exercice :

- Copier [la capture chiffrée avec WEP](#)
- Ouvrir le fichier avec Wireshark et essayer de lire son contenu. Utiliser des filtres d'affichage de protocoles connus (http, icmp). Est-ce que vous arrivez à trouver des trames contenant ces protocoles ? (normalement pas puisque le contenu est chiffré !)
- Utiliser `aircrack-ng` pour récupérer la clé de chiffrement du réseau WEP. Si vous utilisez une distribution Kali, aircrack est déjà installé. Sinon, renseignez-vous sur Internet pour l'installer sur votre système.

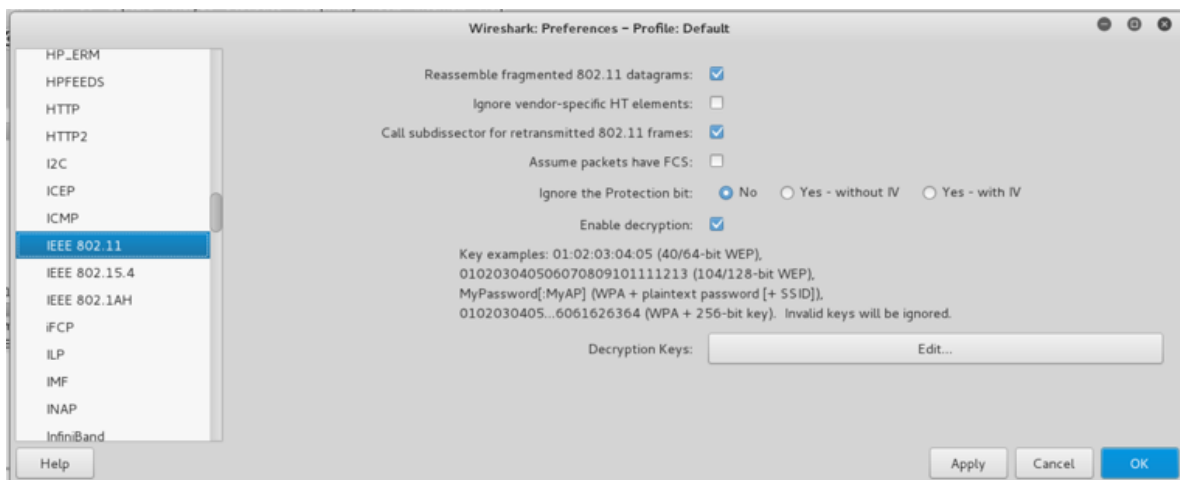
```
aircrack-ng <nom-du-fichier-capture>
```

Maintenant que vous avez la clé WEP, configurez la dans Wireshark afin de déchiffrer le trafic (en fonction de la version de Wireshark, ces images peuvent varier légèrement) :

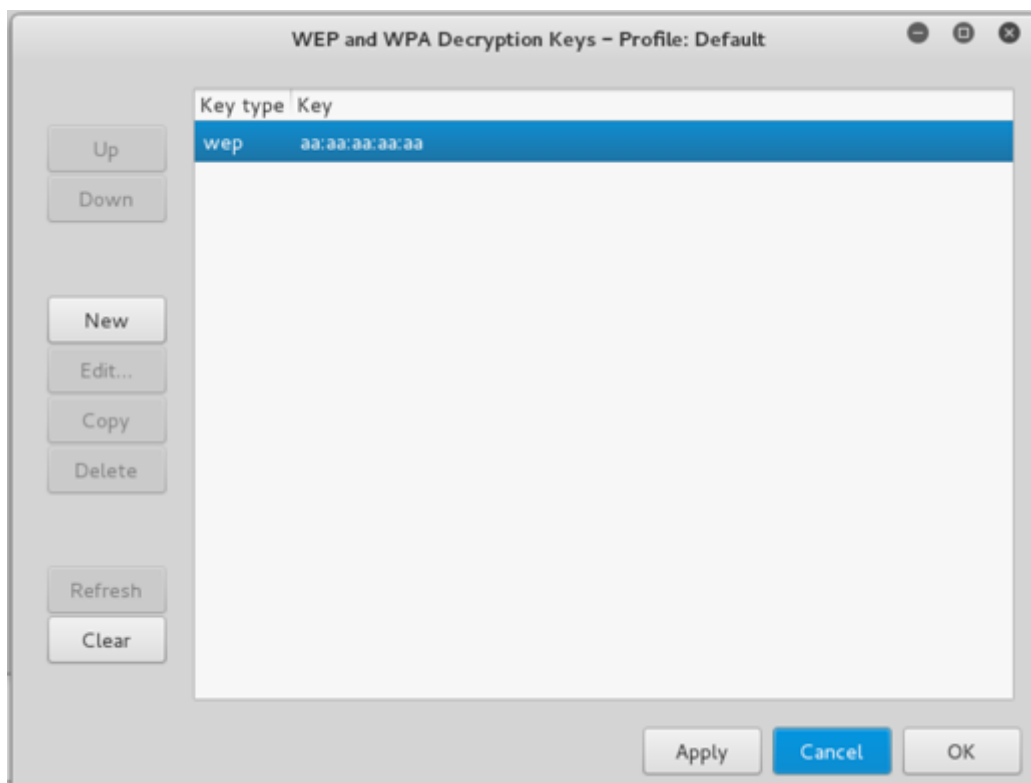
- Ouvrir les préférences de Wireshark et localiser l'option « Protocols »



- Dans « Protocols », trouver le protocole IEEE 802.11. Activer l'option « Enable decryption » et ensuite cliquer sur le bouton « Edit » de la fenêtre pour ajouter une nouvelle clé WEP



- Cliquer sur « New » et entrer la nouvelle clé WEP que vous avez trouvée avec `aircrack`. Puis, accepter :



- Essayez à nouveau de lire le contenu de la capture. Utilisez encore une fois des filtres de protocoles connus (http, icmp). Est-ce que vous arrivez à trouver des trames contenant ces protocoles cette fois-ci ?
- Répondre aux questions suivantes :

Question : Combien de temps avez-vous attendu pour obtenir la clé WEP ?

Réponse : La clé est arrivée instantanément, pas eu de temps d'attente.

Montrer une capture d'écran de l'obtention de la clé WEP

Capture ici

```

Aircrack-ng 1.6
1: wlan.fc.type_subtype == 0x0004

2: fc:f1:36:22:49:74 [00:00:00] Tested 37 keys (got 13604 IVs)

KB  che  depth  byte(vote)
0   0/  1  AB(21248) 64(19200) 11(18688) CC(18432) 70(17920)
1   0/  1  AB(20736) 52(18432) 97(18432) F6(17920) A5(17664)
2   2/  3  AB(18688) 1B(17920) 02(17664) 48(17664) D4(17408)
3   3/  4  CD(19200) 70(18176) 71(18176) 7B(17664) AF(17408)
4   0/  3  4E(19712) 2F(18944) 9B(18944) 00(18432) 9D(18432)

KEY FOUND! [ AB:AB:AB:CD:CD ]
Decrypted correctly: 100%
  
```

Question : Arrivez-vous à récupérer les informations d'identification (credentials) de l'authentification basique http contenue dans la capture ?

Réponse : admin:admin , il faut utiliser le filtre Wireshark http.authorization

Réseaux protégés par WPA

Introduction

La réponse aux problèmes de sécurité de WEP est arrivée sous la forme d'une couche supplémentaire (protocole TKIP) utilisant toujours le moteur de chiffrement de WEP mais le rendant beaucoup plus fort. Un peu plus tard, la norme 802.11i spécifie la nouvelle méthode WPA2, utilisant AES pour le chiffrement et le contrôle de l'intégrité des messages.

Malgré le fait que ces protocoles sont très performants, ils sont vulnérables à des attaques par dictionnaire, à condition de capturer l'authentification d'un utilisateur légitime.

Vous allez exploiter cette faille dans la partie suivante en utilisant la suite aircrack pour trouver une passphrase WPA-PSK.

Travail à réaliser

Exercice Authentification :

Nous utiliserons Wireshark pour trouver l'authentification WPA contenue dans le 4-way handshake.

- Copier [le fichier de capture chiffré avec WPA](#) sur votre machine
- Utiliser Wireshark pour identifier les 4 messages échangés au moment de l'authentification WPA. Vous pouvez utiliser le filtre d'affichage suivant `ea01` de Wireshark
- Analyser les messages du 4-way handshake. En particulier, essayer de trouver les chiffres aléatoires (Nonces) échangés entre le client et l'AP.

Fournir une capture d'écran des chiffres aléatoires

Capture ici

```
WPA Key Nonce: 60cb806f531978f2b6b18d1cad6855e592333764791225fa...
WPA Key Nonce: 72f64cc60d16d2c6f6e61c3ea6a3961f2a9651324918d26f...
WPA Key Nonce: 60cb806f531978f2b6b18d1cad6855e592333764791225fa...
WPA Key Nonce: 72f64cc60d16d2c6f6e61c3ea6a3961f2a9651324918d26f...
```

Exercice déchiffrement WPA :

Nous allons nous servir de l'outil aircrack-ng et d'un dictionnaire pour retrouver la passphrase utilisée pour protéger un réseau dont nous avons une capture. Une fois la passphrase récupérée, nous l'utiliserons dans Wireshark pour rendre la capture lisible.

- Copier [le dictionnaire](#) sur votre machine locale
- Utilisez aircrack-ng en ligne de commandes pour cracker la passphrase du réseau WPA avec le même [fichier de capture chiffrée avec WPA](#) que vous avez déjà copié.

```
aircrack-ng <nom-du-fichier-capture> -w <nom-du-dictionnaire>
```

- Configurer la passphrase WPA dans Wireshark afin de déchiffrer le trafic (utiliser les exemples de la partie WEP comme guide. Sélectionnez « wpa-pwd » comme type de clé)
- Répondre aux questions suivantes :

Question : Combien de temps avez-vous attendu pour obtenir la passphrase WPA ?

Réponse : une dizaine de secondes

Montrer une capture d'écran de l'obtention de la passphrase WPA

Capture ici

```
Aircrack-ng 1.6

[00:00:12] 119121/121460 keys tested (9667.77 k/s)

Time left: 0 seconds 98.07%

KEY FOUND! [ anticonstitutionnellement ]

Master Key : B8 CF 69 D7 12 34 F8 C2 9D 4D 34 EB C7 F2 4F A6
              EF 89 E1 97 6B F7 10 6E EC 62 C6 4A AB A5 8E EC

Transient Key : 39 75 2E FD E0 A2 B6 51 7C FD C6 2F C8 FF A8 68
                80 82 82 62 06 0E 4C 3B DC 82 79 44 34 40 C1 B5
                60 80 F0 F9 68 06 1C E6 D4 BD 68 26 39 AA 7A 79
                3B C1 54 B5 39 9A A6 5F 82 AA 25 72 6D 8A 22 25

EAPOL HMAC : 21 8C C7 CD 4F 28 04 AC F2 72 95 77 D3 98 94 3F
```

Question : Lors de la capture, la cible a fait un « ping » sur un serveur. Arrivez-vous à dire de quel serveur il s'agit ?

Réponse :

Adresse IP du serveur : 31.13.64.35

Nom de Domaine : facebook.com

Il s'agit du serveur de facebook

Exercice déchiffrement WPA 2 :

Nous avons enlevé une seule trame (choisie stratégiquement) du fichier de capture original chiffré avec WPA. On vous demande d'essayer de refaire l'exercice précédent mais avec [ce nouveau fichier de capture](#) utilisant donc [le même dictionnaire](#).

- Répondre aux questions suivantes :

Question : Est-ce que vous arrivez à refaire l'exercice ? Pourquoi ou pourquoi pas ?

Réponse :

Il ne trouve pas de network, probablement parce qu'il manque un message dans le 4way handshake lors de la conversation pour l'authentification.

```
[x]-(diego@parrot)-[~/Downloads]
$aircrack-ng coursWLAN-WPA-filtered.cap -w ../french_dico.txt
Reading packets, please wait...
Opening coursWLAN-WPA-filtered.cap
Unsupported file format (not a pcap or IVs file).
Read 0 packets.

No networks found, exiting.

© 2020 GitHub, Inc. Terms Privacy Security Status Help
Quitting aircrack-ng...
```

Question : Sur la base de votre réponse précédente, arrivez-vous à déduire quelle trame a été effacée ?

Réponse :

Sur la première capture, on observe qu'il y a 4 messages entre Cisco et Apple.

eapol						
No.	Time	Source	Destination	Protocol	Length	Info
591	4.964674	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	131	Key (Message 1 of 4)
593	4.968244	Apple_e5:cf:b9	Cisco-Li_bd:9e:a0	EAPOL	155	Key (Message 2 of 4)
640	5.962114	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	157	Key (Message 3 of 4)
642	5.963636	Apple_e5:cf:b9	Cisco-Li_bd:9e:a0	EAPOL	131	Key (Message 4 of 4)
644	5.965186	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	183	Key (Group Message 1 of 2)
646	5.967220	Apple_e5:cf:b9	Cisco-Li_bd:9e:a0	EAPOL	151	Key (Group Message 2 of 2)

En revanche, sur la deuxième capture on observe qu'il manque le message 2 entre Cisco et Apple.

eapol						
No.	Time	Source	Destination	Protocol	Length	Info
591	4.964674	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	131	Key (Message 1 of 4)
639	5.962114	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	157	Key (Message 3 of 4)
641	5.963636	Apple_e5:cf:b9	Cisco-Li_bd:9e:a0	EAPOL	131	Key (Message 4 of 4)
643	5.965186	Cisco-Li_bd:9e:a0	Apple_e5:cf:b9	EAPOL	183	Key (Group Message 1 of 2)
645	5.967220	Apple_e5:cf:b9	Cisco-Li_bd:9e:a0	EAPOL	151	Key (Group Message 2 of 2)