Table des matières

1) Remise à zéro

a) J'enlève l'alimentation

b) J'appuie sur le bouton de réinitialisation et je branche l'alimentation. J'attend que la didode devienne orange et je relâche

2) Utilisation du port console

a) Je branche le port console entre mon pc et le point d'accès CISCO

b) J'utilise le logiciel putty pour me connecter au point d'accès (port serial)

c) J'appuie plusieurs fois sur la touche entrée pour faire apparaître le mot ap

d) Je tape ensuite en pour passer en mode administrateur (mot de passe : Cisco). Je désactive les log du point d'accès.

```
ap(config)#no logging console
ap(config)#exit
```

e) J'affiche la configuration en cours avec la commande show running-config

f) J'ajoute un SSID en diffusion avec une authentification ouverte avec les commandes suivantes :

```
 ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid 4869
ap(config-ssid)#guest-mode
ap(config-ssid)#authentification open
```

```
                          ^
% Invalid input detected at '^' marker.

ap(config-ssid)#authentication open
ap(config-ssid)#exit
ap(config)#exit
```

g) Je configure maintenant l'interface 802.11g pour utiliser notre SSID et ajoute un channel

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface Dot11Radio0
ap(config-if)#ssid 4869
ap(config-if)#channel 2
ap(config-if)#power local cck -1
ap(config-if)#power-local ofdm -1
                   ^
% Invalid input detected at '^' marker.

ap(config-if)#no shut
ap(config-if)#exit
ap(config)#exit
```

h) Je vérifie qu'un client puisse s'y connecter. Pour cela on récupère le fichier M3101.conf sur moodle et on l'édite. Dedans on modifie la ligne SSID et on met le SSID que nous avons choisis (ici 4869). On ouvre une connexion avec la commande suivante :

```
sudo wpa_supplicant -i wlan0 -c M3101.conf
```

J'affiche ensuite les associations sur l'AP avec la commande suivante :

```
ap>sh dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [4869] :

MAC Address    IP address      Device        Name
Parent         State
b827.eba2.3dd6 0.0.0.0         unknown       -               self
Assoc
```

i) Maintenant je supprime le SSID et je vérifie qu'il se supprime également dans l'interface 802.11g

```
ap#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#no dot11 ssid 4869
ap(config)#exit
```

```
ap#sh dot11 associations
```

j) Je crée maintenant un SSID permettant de mettre en place une clé WPA-PSK avec une clé partagée :

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid 4869
ap(config-ssid)#guest-mode
ap(config-ssid)#authentication open

ap(config-ssid)#authentication key-management wpa
ap(config-ssid)#wpa-psk ascii 0 12345678
ap(config-ssid)#exit
ap(config)#interface Dot11Radio0
ap(config-if)#encryption mode ciphers tkip
ap(config-if)#ssid 4869
ap(config-if)#exit
ap(config)#exit
```

k) Sur le client on vérifie que le scan indique bien WPA-PSK avec un chiffrement TKIP (surligné en bleu)

```
BSS 00:19:07:34:8c:20(on wlan0)
     last seen: 3087.182s [boottime]
     TSF: 0 usec (0d, 00:00:00)
     freq: 2417
     beacon interval: 100 TUs
     capability: ESS Privacy ShortPreamble ShortSlotTime APSD
(0x0c31)
     signal: -38.00 dBm
     last seen: 0 ms ago
     SSID: 4869
     Supported rates: 1.0* 2.0* 5.5* 6.0 9.0 11.0* 12.0 18.0
     DS Parameter set: channel 2
     ERP: <no flags>
     Extended supported rates: 24.0 36.0 48.0 54.0
     WPA:  * Version: 1
           * Group cipher: TKIP
```

```
            * Pairwise ciphers: TKIP
            * Authentication suites: PSK
            * Capabilities: 4-PTKSA-RC 4-GTKSA-RC (0x0028)
     WMM:   * Parameter version 1
            * u-APSD
            * BE: CW 15-1023, AIFSN 3
            * BK: CW 15-1023, AIFSN 7
            * VI: CW 7-15, AIFSN 2, TXOP 3008 usec
* VO: CW 3-7, AIFSN 2, TXOP 1504 usec
```

l) Nous devons connecter le client en utilisant le fichier de configuration. Tout d'abord on modifie le fichier et on le met de la façon suivante :

```
network={
ssid="4869"
auth_alg=OPEN
proto=WPA
key_mgmt=WPA-PSK
pairwise=TKIP
group=TKIP
psk="12345678"
}
```

Après avoir modifié le fichier on relance une connexion et on voit qu'elle est bien établie

m) Sur l'AP je passe en version WPA2 sur l'interface 802.11g grâce à la commande suivante :

```
ap(config-if)#encryption mode ciphers aes-ccm
```

n) Maintenant on adapte le fichier de configuration pour tester le nouveau système (les valeurs modifiées sont surlignées en bleu) :

```
network={
ssid="4869"
auth_alg=OPEN
proto=RSN
key_mgmt=WPA-PSK
pairwise=CCMP
group=CCMP
psk="12345678"
}
```

3) Le mode WPA/WPA2-Entreprise

a) On récupère les fichiers de configuration sur l'ENT que l'on transfère ensuite dans la raspi. On édite ensuite le fichier eap-mschapv2.conf de la façon suivante :

```
network={
eapol_flags=0
key_mgmt=NONE
eap=MSCHAPV2
identity="bob"
password="hello"
}
```

Une fois le fichier édité de cette façon nous lançon la commande suivante pour tester les protocoles :

```
sudo ./eapol_test-2.9-arm64 -a 10.205.20.1 -s testing123 -c eap-
mschapv2.conf
```

b) On test maintenant avec le protocole on EAP-TTLS-MSCHAPV2. D'abord on modifie le fichier eap-ttls-mschapv2.conf pour le mettre de la façon suivante :

```
network={
eapol_flags=0
key_mgmt=NONE
eap=TTLS
anonymous_identity="anonymous"
identity="bob"
password="hello"
phase2="auth=MSCHAPV2"
}
```

Maintenant on relance la commande précédente en mettant le bon fichier :

```
sudo ./eapol_test-2.9-arm64 -a 10.205.20.1 -s testing123 -c eap-
ttls-mschapv2.conf
```

4) Utilisation de l'interface web de l'AP

a) J'attribue une adresse IP au point d'accès grâce aux commandes suivantes :

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface bvi1
ap(config-if)#ip address 10.205.15.3 255.255.0.0
ap(config-if)#exit
ap(config)#ip default-gateway 10.205.255.254
ap(config)#exit
ap#write
Building configuration...
[OK]
```

b) On branche le point d'accès au réseau local

c) On test la connexion entre plusieurs points :

Du PC vers l'AP :

```
samuel.laforge01@205-15 ~ $ ping 10.205.15.3
PING 10.205.15.3 (10.205.15.3) 56(84) bytes of data.
64 bytes from 10.205.15.3: icmp_seq=1 ttl=255 time=1.19 ms
64 bytes from 10.205.15.3: icmp_seq=2 ttl=255 time=0.670 ms
^C
--- 10.205.15.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.670/0.933/1.197/0.265 ms
```

De l'AP vers le PC :

```
ap#ping 10.205.15.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.205.15.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1
ms
```

De l'AP vers internet :

```
ap#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7
ms
```

d) Maintenant on ouvre une page web et en URL on met l'IP de l'AP (ici 10.205.15.3)

Une fois sur la page d'authentification on ne donne que le mot de passe qui est Cisco

e) On affiche la configuration actuelle de l'AP qui se situe dans le menu System Software + System Configuration + fichier cong.txt :

f) On configure le serveur Radius qui se situe dans le menu SECURITY + Server Manager + Corporate servers. On met l'ip du serveur qui est 10.205.20.1, secret = testing123, ports = 1812 et 1813

g) Toutes les lignes qui commencent par «aaa» sont apparues