Compte Rendu TP3 M3101

Table des matières

1. Capture de trames.....1
2. Chiffrement TKIP.....6

1. Capture de trames

Je regarde si la carte est en mode monitor

Je tape iw dev

```
pi@pi205-2:~ $ iw dev
phy#0
	Interface wlan0
		ifindex 3
		wdev 0x1
		addr b8:27:eb:04:04:9d
		type managed
		channel 1 (2412 MHz), width: 20 MHz, center1: 2412 MHz
```

Son type est « managed » donc elle n'est pas en monitor

On voit avec iw phy qu'elle ne supporte pas le type monitor

```
Supported RX frame types:
		 * managed: 0x40 0xd0
		 * P2P-client: 0x40 0xd0
		 * P2P-GO: 0x00 0x20 0x40 0xa0 0xb0 0xc0 0xd0
* P2P-device: 0x40 0xd0
```

b. Je fais un scan des points d'accès WiFi (J'active ma carte WiFi au préalable)

Je vois bien le point d'accès IUTBEZIERS

```
BSS 00:3a:9a:24:5b:53(on wlan0)
     last seen: 1158.186s [boottime]
     TSF: 0 usec (0d, 00:00:00)
     freq: 2462
     beacon interval: 100 TUs
     capability: ESS ShortPreamble ShortSlotTime (0x0421)
     signal: -86.00 dBm
     last seen: 0 ms ago
     SSID: IUTBEZIERS
```

je crée un fichier pour me connecter au réseau avec IUTBEZIERS comme SSID

```
network={
ssid="IUTBEZIERS"
auth_alg=OPEN
key_mgmt=NONE
}
```

Je suis connecté, je regarde avec la commande iw wlan0 link

```
root@pi205-2:/home/pi# iw wlan0 link
Connected to 00:3a:9a:24:58:e3 (on wlan0)
     SSID: IUTBEZIERS
     freq: 2412
```

Elle me dit que je suis bien connecté.

Je fais alors une requête DHCP pour la carte wlan0

```
root@pi205-2:/home/pi# dhclient -v wlan0
...
bound to 172.31.0.76 -- renewal in 258 seconds.
```

```
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000
    link/ether b8:27:eb:04:04:9d brd ff:ff:ff:ff:ff:ff
    inet 172.31.0.76/16 brd 172.31.255.255 scope global dynamic
wlan0
```

On voit que l'adresse qui m'est donnée est bien celle de la requête DHCP

c. On fait les commandes données

On voit bien en faisant id qu'on appartient au groupe wireshark.

d.

On sniffe les données et on voit qu'aucune trame 802.11 passe

```
pi@pi205-1:~ $ tshark -ni wlan0
Capturing on 'wlan0'
    1 0.000000000  172.31.0.97 ? 172.31.0.1   ICMP 98 Echo (ping)
request  id=0x0679, seq=16/4096, ttl=64
    2 0.005734563   172.31.0.1 ? 172.31.0.97  ICMP 98 Echo (ping)
reply    id=0x0679, seq=16/4096, ttl=64 (request in 1)
    …
```

e. On brancha la clé WiFi. On la passe en mode monitor avec la commande

iw wlan1 set type monitor

On réactive la carte avec la commande : ip link set up dev wlan1

On voit bien les trames qui passent sur le réseau.

J'en prends une au hasard (Elles sont toutes en 802.11 de toute manière)

```
No.     Time           Source                Destination
Protocol Length Info
     19 0.516620214    Cisco_24:58:e5        Broadcast
802.11   245

Frame 19: 245 bytes on wire (1960 bits), 245 bytes captured (1960
bits) on interface 0
Radiotap Header v0, Length 36
802.11 radio information
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 1,0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -90dBm
    TSF timestamp: 105173213985
```

On voit bien que la machine envoie des données et qu'on les récupère en 802.11

f. On enregistre ce que l'on voit grâce à l'option -w de tshark.

On voit alors plusieurs types de 802.11 :

- Beacon Frame

- Probe Request

- Probe Response

- QoS

- Acknowledgement

- Clear-to-send

```
No.     Time           Source                Destination
Protocol Length Info
     53 1.264979656                           Cisco_24:58:e3
(00:3a:9a:24:58:e3) (RA) 802.11   50     Acknowledgement,
Flags=...P....C

No.     Time           Source                Destination
Protocol Length Info
     52 1.264659397    Cisco_24:58:e3        Raspberr_04:04:9d
802.11   220    Probe Response, SN=2611, FN=0, Flags=........C,
BI=100, SSID=IUTBEZIERS

No.     Time           Source                Destination
Protocol Length Info
     51 1.262948573    Raspberr_04:04:9d     Broadcast
802.11   260    Probe Request, SN=991, FN=0, Flags=........C,
SSID=IUTBEZIERS

No.     Time           Source                Destination
Protocol Length Info
     49 1.257862349    Raspberr_04:04:9d     Cisco_24:58:e3
802.11   66     QoS Null function (No data), SN=990, FN=0,
Flags=...P...TC

No.     Time           Source                Destination
Protocol Length Info
     48 1.253315966    Cisco_24:58:e6        Broadcast
802.11   239    Beacon frame, SN=2610, FN=0, Flags=........C,
BI=100, SSID=\000

No.     Time           Source                Destination
Protocol Length Info
     67 1.480509280                           Broadcom_04:04:9d
(e0:3e:44:04:04:9d) (RA) 802.11   50     Clear-to-send,
Flags=........C
```

g. Pour voir le canal utilisé par la carte wlan0, on fait : iw dev

```
Interface wlan0
          ...
          type managed
          channel 1 (2412 MHz), width: 20 MHz, center1: 2412 MHz
```

On change le canal d'écoute sur la clé WiFi

```
pi@pi205-1:~ $ sudo iw wlan1 set channel 1
```

h. Je fais un ping sur un autre rapsberry

Le mien à comme IP : 172.31.0.76

```
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000
    link/ether b8:27:eb:04:04:9d brd ff:ff:ff:ff:ff:ff
    inet 172.31.0.76/16 brd 172.31.255.255 scope global dynamic
wlan0
```

```
No.     Time           Source                Destination
Protocol Length Info
     16 1.008443966    172.31.0.76           172.31.0.244
ICMP     158    Echo (ping) request  id=0x053f, seq=7/1792, ttl=64
(reply in 18)

IEEE 802.11 QoS Data, Flags: ....R..TC
    Type/Subtype: QoS Data (0x0028)
    ...
Internet Protocol Version 4, Src: 172.31.0.76, Dst: 172.31.0.244
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    ...
    Data (48 bytes)
```

On voit que c'est une trame 802.11 et on voit que c'est un ping

i. On peut utiliser la commande suivant avec tshark :

tshark -r NOM_FICHIER -Y « eth.addr == ADRESSE_MAC »

j. On peut utiliser la commande suivant sous tshark :

tshark -r NOM_FICHIER -Y wlan_mgt.ssid == «SSID »

2. Chiffrement TKIP

a. On fait un scan du réseau avec notre interface WiFi

```
BSS 00:19:07:34:8a:20(on wlan0)
     last seen: 3949.863s [boottime]
     TSF: 0 usec (0d, 00:00:00)
     freq: 2442
     DS Parameter set: channel 7
     ...
     last seen: 0 ms ago
     SSID: WPA-PSK
* Group cipher: TKIP
```

On voit que ce point d'accès est bien WPA-PSK et que son type de chiffrement est le TKIP

c. On voit 4 trames avec notre adresse MAC

```
  137 2.891251914 00:19:07:34:8a:20 ? b8:27:eb:04:04:9d EAPOL 173
Key (Message 1 of 4)
  138 2.891723892 00:19:07:34:8a:20 ? b8:27:eb:04:04:9d EAPOL 173
Key (Message 2 of 4)
 140 2.894469300 b8:27:eb:04:04:9d ? 00:19:07:34:8a:20 EAPOL 197
Key (Message 2 of 4)
  142 2.895395912 00:19:07:34:8a:20 ? b8:27:eb:04:04:9d EAPOL 199
Key (Message 3 of 4)
  144 2.897131272 b8:27:eb:04:04:9d ? 00:19:07:34:8a:20 EAPOL 173
Key (Message 4 of 4)
```

Elles montrent la connexion chiffrée

d. On n'arrive pas à voir les trames :

Display filters were specify both with -d (On n'utilise pas -d)

Si on laisse seulement (wlan.fc.type==2), on voit qu'il nous remontre les connexions chiffrées

On voit la data qu'on envoie (ping)

```
root@pi205-2:/home/pi# ping -I wlan0 10.205.255.254
PING 10.205.255.254 (10.205.255.254) from 10.205.0.172 wlan0:
56(84) bytes of data.
64 bytes from 10.205.255.254: icmp_seq=1 ttl=255 time=10.10 ms
64 bytes from 10.205.255.254: icmp_seq=2 ttl=255 time=5.56 ms
```

187 3.661149821 00:19:2f:a6:ab:ec ? b8:27:eb:04:04:9d 802.11 140 QoS Data, SN=695, FN=0, Flags=.p....F.C

```
  201 3.783547128 b8:27:eb:04:04:9d ? 01:00:5e:00:00:fb 802.11 126
QoS Data, SN=0, FN=0, Flags=.p.....TC
  222 3.900862939 00:19:2f:a6:ab:ec ? b8:27:eb:04:04:9d 802.11 144
QoS Data, SN=696, FN=0, Flags=.p....F.C
...
```

C’est bien mon adresse MAC

e. On modifie les fichiers comme montré dans le sujet.