Analyse d'une probe request

1 - Objectif

L'objectif de cette issue est de comprendre le contenu d'une Probe Request émise par un périphérique WI-FI, et déterminer comment la capturer pour l'analyser.

2 - Principe

Une probe request utilise une trame 802.11 envoyé par un client Wi-FI (smartphone, PC...) pour rechercher des points d'accès disponible.

3 - Capture d'une Probe request

a) Est ce possible ?

Oui, il est possible de capturer des Probe Requests à condition que la carte Wi-Fi supporte le mode “monitor” (mode écoute passive).
Aucune carte spéciale n’est requise, mais toutes ne sont pas compatibles.

b) Mise en place de l'environnement (Kali Linux)

1 - Lister les interfaces disponible

```
ip link show
```

2 - Arrêter les services réseau susceptibles de gêner

```
sudo systemctl stop NetworkManager
sudo systemctl stop wpa_supplicant
sudo airmon-ng check kill
```

3 - Passer l’interface en mode monitor

```
sudo ip link set wlan0 down
sudo iw dev wlan0 set type monitor
sudo ip link set wlan0 up
```

4 - Vérifier le mode

```
iw dev
```

Revenir en mode Managed (mode par défaut)

```
sudo ip link set wlan0 down
sudo iw dev wlan0 set type managed
sudo ip link set wlan0 up
sudo systemctl start NetworkManager
sudo systemctl start wpa_supplicant
```

Vérification

```
iwconfig
```

c) Capture avec Wireshark

- Lancer Wireshark
- Sélectionner l'interface qui est en mode monitor
- Appliquer le filtre suivant pour afficher uniquement les Probe Requests.

```
  wlan.fc.type_subtype == 0x04
```

- Filtrer par source :

```
wlan.sa == 12:34:56:78:9a:bc
```

d) Contenu d'une Probe Request

En-tête de trame (Frame Header)

Champ	Description	Taille (octets)
Frame Control	Version, type, sous-type (ici : Probe Request), flags de contrôle	2
Duration / ID	Temps réservé pour la trame ou identifiant	2
Address 1 (Destination)	Adresse MAC de destination (souvent broadcast `ff:ff:ff:ff:ff:ff`)	6
Address 2 (Source)	Adresse MAC du client émetteur	6
Address 3 (BSSID)	Identifiant du point d’accès ou broadcast	6
Sequence Control	Numéro de séquence pour ordonnancement des trames	2

Corps de trame (Information Elements)

Ordre	Élément	Description
1	**SSID**	Identifiant du réseau recherché ou “ANY” (recherche ouverte)
2	**Supported Rates**	Liste des débits supportés par le client
3	**Request Information**	Demande d’éléments d’information à l’AP
4	**Extended Supported Rates**	Débits supplémentaires supportés
5	**DSSS Parameter Set**	Paramètres d’étalement du spectre
6	**Supported Operating Classes**	Classes de fonctionnement supportées
7	**HT Capabilities**	Capacités “High Throughput” (802.11n)
8	**20/40 BSS Coexistence**	Coexistence de réseaux 20/40 MHz
9	**Extended Capabilities**	Options avancées (QoS, sécurité, etc.)
10	**SSID List**	Liste de SSID recherchés simultanément
11	**Channel Usage**	Informations sur l’utilisation des canaux
12	**Interworking**	Compatibilité multi-réseaux (802.11u)
13	**Mesh ID**	Identifiant du réseau maillé
14	**VHT Capabilities**	Capacités “Very High Throughput” (802.11ac)
15	**Power Capability**	Plage de puissance d’émission supportée
16	**Supported Channels**	Liste des canaux supportés
17	**Mobility Domain**	Gestion de mobilité (802.11r)
18	**Timeout Interval**	Délais de temporisation
19	**Fast BSS Transition**	Support des transitions rapides entre AP
Dernier	**Vendor Specific**	Champs propriétaires (Apple, Samsung, etc.)

Pied de trame

Champ	Description	Taille (octets)
Frame Check Sequence (FCS)	Code CRC sur 4 octets, pour vérifier l’intégrité du paquet. Si le CRC ne correspond pas, la trame est rejetée.	4