Write-up WiFi-labo

Table of contents

Intro

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked phrase by Wi-Fi Alliance that means IEEE 802.11x.

Modes of WiFi

In the 802.11x protocol, each device can be in one of 6 modes.

Master mode

This is the mode you'll usually find an access point in. In this mode, the device cannot connect to an access point. It can only serve as a connection point for other devices.

Managed mode

This is the most common mode, as it is the mode that is used by almost every client device (laptops, smartphones, fridges, ...). Only from this mode, the device can connect to an access point running in master mode. The connection between a master mode and a connection mode is by far the most common one.

Others

There are some other, less common modes as well. Most of these could appear in day to day use, but some are hardly ever seen.

Repeater mode

In this mode, the device will "extend" a network by taking all the packets it receives and broadcasting them again.

Ad-Hoc mode

A peer-to-peer connection. Devices are directly connected to eachother. This is obviously not suitable for day-to-day use, but is convenient for some use-cases, such as ad-hoc gaming.

Mesh mode

Ad-hoc on steroids. In this mode, devices will all be connected to eachother in a mesh. If one of the devices fails, the other clients will be able to re-route traffic along other devices.

Monitor mode

In this mode you can not connect to other devices, but the device can 'monitor' all the frames that are sent over the air.

> **What modes does my adapter support**
>
> **Bash**
>
> ```
> iw list | grep -A 8 modes:
> ```
>
> This command will list all the modes for your NIC

Management frames

The 802.11x has three types of frames. Management-frames, control-frames and data-frames.

Beacon frames

An access point constantly broadcasts beacon frames to advertise itself.

example.pcap

The file above is a capture made in monitor mode. This means that it captures all of the packets sent over the air during the time of capture, of all devices in range.

When we open it contains a big amount of frames, but for now, we are only interested in the 'Beacon frames'. For this we apply the following filter:

Wireshark Beacon Frame filter

```
wlan.fc.type_subtype == 0x08
```

This results in a big list of beacon frames, looking somewhat like this:

9	0.024753	Apple_d1:b5:6a	Broadcast	802.11	252 Beacon frame, SN=541, FN=0, Flags=........, BI=100, SSID=PolyExtreme
10	0.028328	6a:15:90:08:c2:8e	Broadcast	802.11	224 Beacon frame, SN=1327, FN=0, Flags=........, BI=100, SSID=PROXIMUS_AUTO_FON
84	0.120665	Sagemcom_08:c1:8c	Broadcast	802.11	251 Beacon frame, SN=1328, FN=0, Flags=........, BI=100, SSID=WiFi-2.4-c186
85	0.122387	6a:15:90:08:c2:8d	Broadcast	802.11	197 Beacon frame, SN=1329, FN=0, Flags=........, BI=100, SSID=PROXIMUS_FON
86	0.124415	Apple_d1:b5:6a	Broadcast	802.11	252 Beacon frame, SN=542, FN=0, Flags=........, BI=100, SSID=PolyExtreme
153	0.204868	Cisco-Li_3a:cf:90	Broadcast	802.11	121 Beacon frame, SN=2666, FN=0, Flags=........, BI=100, SSID=Tiebevn
163	0.224509	Sagemcom_08:c1:8c	Broadcast	802.11	251 Beacon frame, SN=1332, FN=0, Flags=........, BI=100, SSID=WiFi-2.4-c186
164	0.226623	Apple_d1:b5:6a	Broadcast	802.11	252 Beacon frame, SN=543, FN=0, Flags=........, BI=100, SSID=PolyExtreme
165	0.228498	6a:15:90:08:c2:8e	Broadcast	802.11	224 Beacon frame, SN=1334, FN=0, Flags=........, BI=100, SSID=PROXIMUS_AUTO_FON
223	0.307334	Cisco-Li_3a:cf:90	Broadcast	802.11	121 Beacon frame, SN=2667, FN=0, Flags=........, BI=100, SSID=Tiebevn
228	0.325367	Sagemcom_08:c1:8c	Broadcast	802.11	251 Beacon frame, SN=1335, FN=0, Flags=........, BI=100, SSID=WiFi-2.4-c186
229	0.327104	6a:15:90:08:c2:8d	Broadcast	802.11	197 Beacon frame, SN=1336, FN=0, Flags=........, BI=100, SSID=PROXIMUS_FON

If we look at the details of a frame, we can see what data it transmits.

```
Frame 153: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
      Timestamp: 0x00000343a74543a4
      Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0411
  Tagged parameters (67 bytes)
    Tag: SSID parameter set: Tiebevn
        Tag Number: SSID parameter set (0)
        Tag length: 7
        SSID: Tiebevn
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 6
    Tag: CF Parameter set: CFP count 0: CFP Period 2: CFP Max Duration 0: CFP Dur Remaining 0
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: ERP Information
    Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    Tag: RSN Information
```

It tells us the SSID (network name), the supported data-rates, the MAC-address of the access point, channel, security,...

When a client device receives this broadcast, it will check if the SSID included in this broadcast is a known network. If so, the device will automatically connect.

Probe requests and responses

Similar to beacon frames, a client device may send out probe requests. In this case, the client will ask if a network is around. In this frame, an SSID is included. If an access point using said SSID receives this frame, it will respond with a probe response. This probe response includes the access point capabilities.

Now try to analyse a probe request and a probe response.

Wireshark Probe Frame filter

```
wlan.fc.type_subtype == 0x04 or wlan.fc.type_subtype == 0x05
```

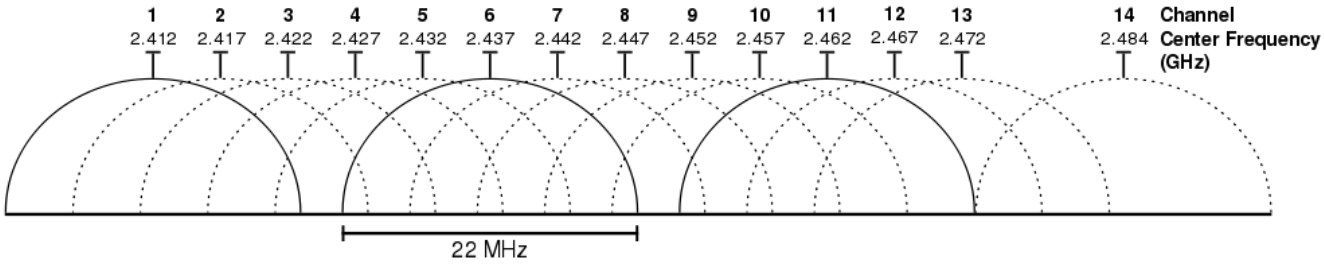
Exploiting probe request/response

Probe-requests can easily be exploited. The system relies on an access point responding when it receives a probe request with it's SSID. However, theoretically anyone can respond to these. There are devices such as the WiFi-pineapple that have the functionality of being a "yes-sayer", meaning they'll respond to any probe request they receive, saying they are the network, when in fact they are not. Because of this, they can get any device to connect to them, and preform man-in-the-middle-attacks.

Channels

WiFi runs on radiosignals. It usually runs in 2 frequencies: the 2.4GHz band, and the 5Ghz band. For the sake of simplicity, we'll focus on the 2.4GHz band.

The 2.4GHz band is divided in 11 channels. A channel is a part of the spectrum, each having a width of 22 MHz. Because of this, all of these channels have an overlap, which causes interference on the network. That is why conventionally, only 3 channels are used, being channel number 1, number 6 and number 11. You'll notice on the picture below that these 3 channels do not have any overlap, because they are spread out.



5Ghz channels

In 5GHz we also have channels, but there are a lot more channels without overlap (23). The reason we're not ditching 2.4GHz alltogether is because 5GHz isn't great when it comes to range, especially through walls. This is why you see more and more 5GHz setups at enterprise level, where there is an access point in each room, but not quite as much in an home-setup, where there usually is only one access point in the basement.

Channel availability

In the US, only channels 1-11 are regulated. All others are not allowed. In the rest of the world, people can use channels 1-13. Only channel 14 is reserved for Japan.

Interference

The 2.4 GHz band is not only used for WiFi. It's also used for microwaves, walkie-talkies, bluetooth... This means is why it is never a good idea to put an access point on a microwave.

Handy links

Reference to 802.11 Wireshark filters

https://www.semfionetworks.com/uploads/2/9/8/3/29831147/wireshark_802.11_filters_-_reference_sheet.pdf

References

https://www.webopedia.com/TERM/W/Wi_Fi.html