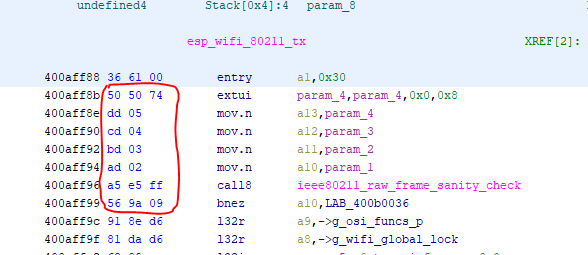
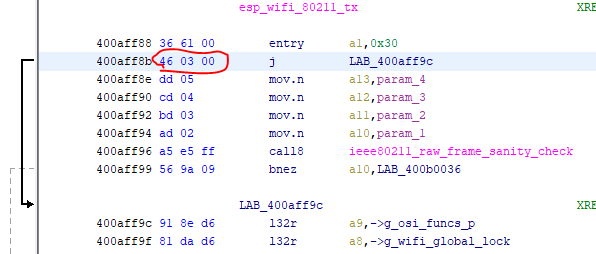
Разработчики SDK espressif, решили ограничить отправку произвольных пакетов, путём добавления функции **ieee80211\_raw\_frame\_sanity\_check** проверки типа пакета (кадра), в функцию **esp\_wifi\_80211\_tx, а** я решил исправить это ограничение. В данном примере рассматривается ESP-IDF 4.3.

Для того чтобы обойти это ограничение, необходимо исправить готовый образ или исполняемый файл elf вашего проекта.

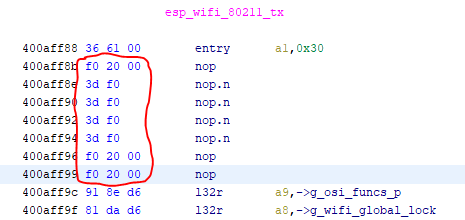
Необходимо найти и исправить последовательность опкодов (\*на ваше усмотрение):



так:



или просто:

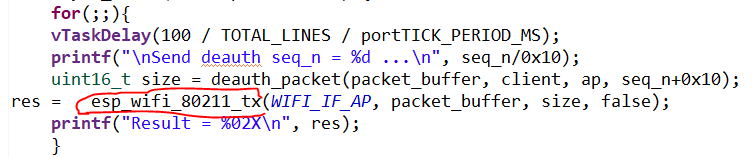


\* на ваше усмотрение – имеются ввиду варианты логики

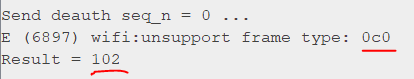
Для получения образа прошивки (для последующей загрузки в память ESP-32) используется утилита esptool с параметрами:

esptool.py --chip esp32 elf2image my\_esp32\_app.elf

Результаты:



до (вывод в монитор порта):



после исправления:



Как уже упоминалось, основная проверка производится в функции **ieee80211\_raw\_frame\_sanity\_check**, которая находится в объектном файле **ieee80211\_output.o** библиотеки **libnet80211.a,** её исправление, позволит собирать последующие проекты без ограничений на тип отправляемого пакета (кадра).

В моём случае, необходимо было проверить **возможность** отправки deauth пакетов в обход ограничения.

Исправление проверено на версии ESP-IDF 4.3, модуля ESP-32, но я думаю, что этот вариант применим и к предыдущим версиям (имеется ввиду обход **ieee80211\_raw\_frame\_sanity\_check**).

Использованные инструменты:

Ghidra

https://ghidra-sre.org/

ghidra-xtensa

https://github.com/yath/ghidra-xtensa