如何从空口抓包中分析终端可协商802.11的最高能力级

wlan接入 **shawccccc** 2023-08-14 发表

问题描述

如何从空口抓包中分析终端可协商802.11的最高能力级

过程分析

HE Capabilities字段 HE代表高效率的，简写是802.11AX的代名词
VHT代表802.11AC HT代表802.11N

断开重连的过程：

1、终端发起解关联请求；

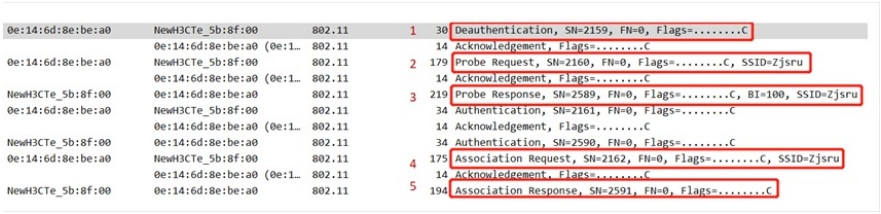
2、终端发起探测请求：这时终端携带了HE—802.11ax能力集；

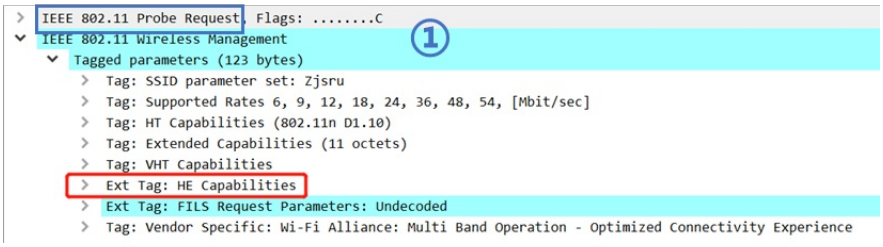
3、AP回复探测请求：AP回复其也支持HE—802.11ax的能力；

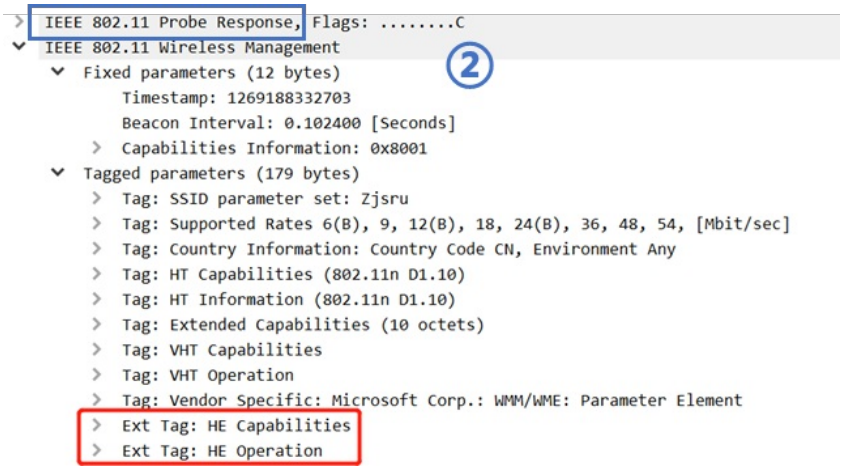
4、终端发起关联请求：终端携带了HE—802.11ax能力集；

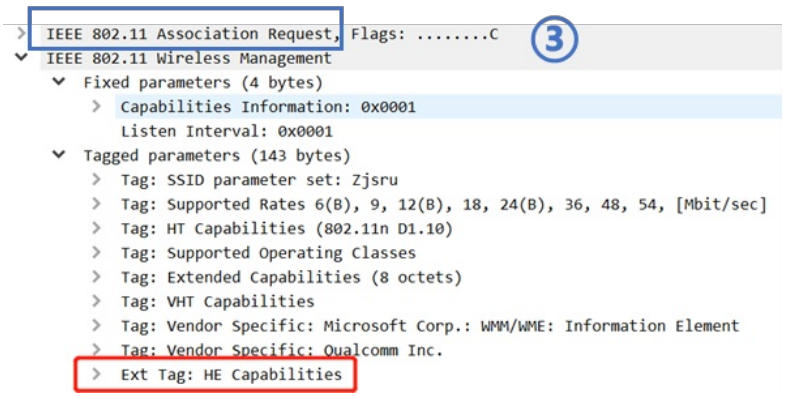
5、AP回复关联请求：AP回复HE—802.11ax能力集请求；

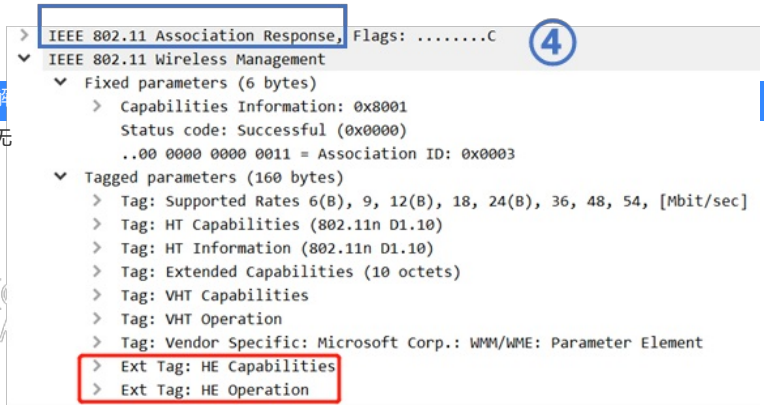
=====》因此终端连接成功后显示了802.11ax的协议










IEEE 802.11 Association Response, Flags: C
4
IEEE 802.11 Wireless Management
Fixed parameters (6 bytes)
Capabilities Information: 0x8001
Status code: Successful (0x0000)
..00 0000 0000 0011 = Association ID: 0x0003
Tagged parameters (160 bytes)
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (10 octets)
Tag: VHT Capabilities
Tag: VHT Operation
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
Ext Tag: HE Capabilities
Ext Tag: HE Operation