

知 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

0e:14:6d:8e:be:a0	NewH3CTe_5b:8f:00	802.11	1	30	Deauthentication, SN=2150, FN=0, Flags=.....C
0e:14:6d:8e:be:a0	0e:14:6d:8e:be:a0 (0e:14:6d:8e:be:a0)	802.11	14	14	Acknowledgement, Flags=.....C
0e:14:6d:8e:be:a0	NewH3CTe_5b:8f:00	802.11	2	179	Probe Request, SN=2160, FN=0, Flags=.....C, SSID=Zjsru
0e:14:6d:8e:be:a0	0e:14:6d:8e:be:a0 (0e:14:6d:8e:be:a0)	802.11	14	14	Acknowledgement, Flags=.....C
NewH3CTe_5b:8f:00	0e:14:6d:8e:be:a0	802.11	3	219	Probe Response, SN=2589, FN=0, Flags=.....C, B1=100, SSID=Zjsru
0e:14:6d:8e:be:a0	NewH3CTe_5b:8f:00	802.11	34	34	Authentication, SN=2161, FN=0, Flags=.....C
0e:14:6d:8e:be:a0	0e:14:6d:8e:be:a0 (0e:14:6d:8e:be:a0)	802.11	14	14	Acknowledgement, Flags=.....C
NewH3CTe_5b:8f:00	0e:14:6d:8e:be:a0	802.11	34	34	Authentication, SN=2590, FN=0, Flags=.....C
0e:14:6d:8e:be:a0	NewH3CTe_5b:8f:00	802.11	4	175	Association Request, SN=2162, FN=0, Flags=.....C, SSID=Zjsru
0e:14:6d:8e:be:a0	0e:14:6d:8e:be:a0 (0e:14:6d:8e:be:a0)	802.11	14	14	Acknowledgement, Flags=.....C
NewH3CTe_5b:8f:00	0e:14:6d:8e:be:a0	802.11	5	194	Association Response, SN=2591, FN=0, Flags=.....C

```
> IEEE 802.11 Probe Request, Flags: .....C
  IEEE 802.11 Wireless Management
    Tagged parameters (123 bytes)
      Tag: SSID parameter set: Zjsru
      Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
      Tag: HT Capabilities (802.11n D1.10)
      Tag: Extended Capabilities (11 octets)
      Tag: VHT Capabilities
      Ext Tag: HE Capabilities
      Ext Tag: FILS Request Parameters: Undecoded
      Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience
```

```
> IEEE 802.11 Probe Response, Flags: .....C
  IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
      Timestamp: 1269188332703
      Beacon Interval: 0.102400 [Seconds]
      Capabilities Information: 0x8001
    Tagged parameters (179 bytes)
      Tag: SSID parameter set: Zjsru
      Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag: Country Information: Country Code CN, Environment Any
      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
```

```
> IEEE 802.11 Association Request, Flags: .....C
  IEEE 802.11 Wireless Management
    Fixed parameters (4 bytes)
      Capabilities Information: 0x0001
      Listen Interval: 0x0001
    Tagged parameters (143 bytes)
      Tag: SSID parameter set: Zjsru
      Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag: HT Capabilities (802.11n D1.10)
      Tag: Supported Operating Classes
      Tag: Extended Capabilities (8 octets)
      Tag: VHT Capabilities
      Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
      Tag: Vendor Specific: Qualcomm Inc.
      Ext Tag: HE Capabilities
```

解
无

- > 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

