某局点三星S7关联协商成单流问题处理经验案例

wlan接入 朱恺 2017-05-24 发表

一、组网

某局点使用无线控制器WX5560H配置多种11AC WAVE2款型AP进行无线覆盖，包括WA5320、WA5620等，同时也有前期cisco无线11AC WAVE1的产品部署。

二、问题描述

三星S7终端关联11AC WAVE2 AP 5G radio时，一直协商成单流的速率能力。现场使用20Mhz频宽的11AC，按照RFC标准，20Mhz，400nsGI的协商在2X2模式下应该为173.3Mbps，但是现场却协商成了86Mbps为1X1的单流模式。如图1：

图1

反复在WAVE2产品上测试比如wa5320、wa5620，效果均一致。强制AP的radio type到11AN终端则能够正常的协商20Mhz的2X2速率144M了；但是在cisco wave1的产品上协商却是正常的2X2上，如图2：

图2

三、过程分析

之前的初步分析判断是由于三星S7的协商能力与H3C的wave2产品存在一定的兼容性问题。因此尝试在AP隐藏模式输入ar5 1 mu disable进行关闭mu-mimo操作。同时对三星S7与5320及三星S7与cisco AP关联进行空口抓包，获取关联过程完整的信息：

1.三星S7与H3C 5320关联请求报文：

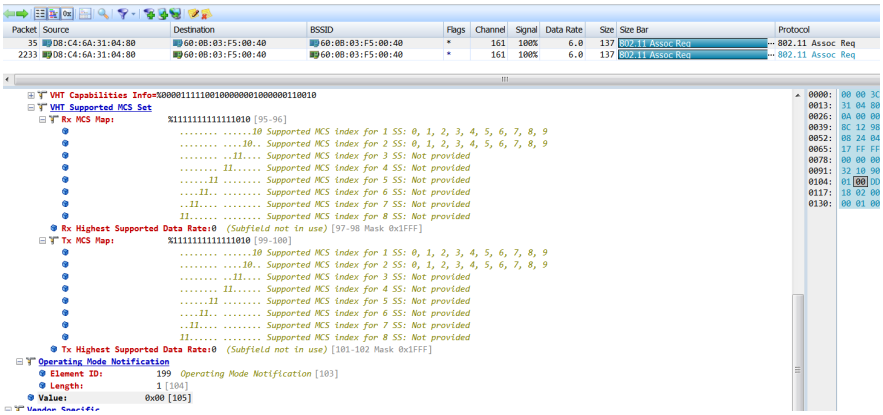

图3

如图3，在终端S7发送的关联请求报文中，Operating Mode Notification字段的Value为0x00，按照RFC标准这里的0代表1条空间流的意思；但是在VHT Supported MCS Set上一直通告的是2SS即2条空间流。这样两处通报能力不一致，在华三无线的处理方式上是按照最小能力去协商的，即现场协商成单流86.7M。

2.三星S7与CISCO AP关联请求报文：

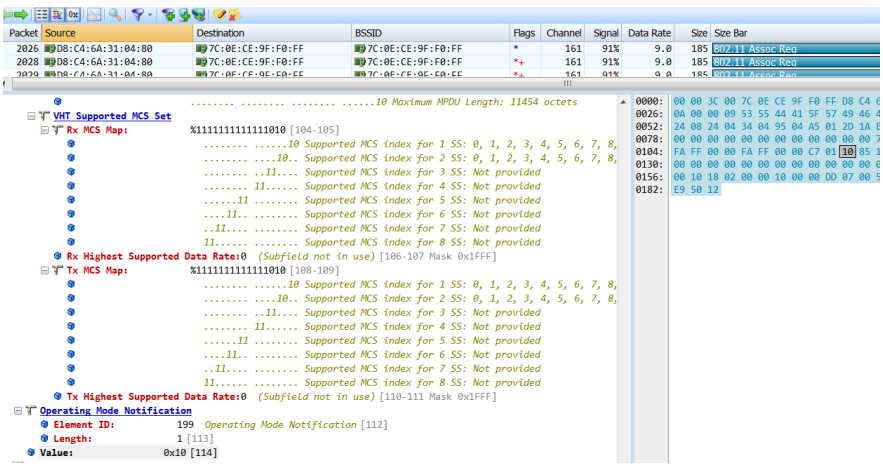

图4

如图4，在终端S7发送的关联请求报文中，Operating Mode Notification字段的Value为0x10，；比且在VHT Supported MCS Set上通告的是2SS即2条空间流。即现场协商成双流173M。

通过上述对比发现三星S7收集在发送能力集的时候与H3C产品发生的关联请求报文出现了前后能力通

报不一致的情况。此时报文中的Operating mode 字段里，Rx Nss Type=0，Rx Nss=1，表示终端支持2条流。

802.11协议对operating mode字段的规定如下（图5）

Table 8-53k—Subfield values of the Operating Mode field

Subfield	Description
Channel Width	If the Rx NSS Type subfield is 0, indicates the supported channel width: Set to 0 for 20 MHz Set to 1 for 40 MHz Set to 2 for 80 MHz Set to 3 for 160 MHz or 80+80 MHz Reserved if the Rx NSS Type subfield is 1.
Rx NSS	If the Rx NSS Type subfield is 0, indicates the maximum number of spatial streams that the STA can receive. If the Rx NSS Type subfield is 1, indicates the maximum number of spatial streams that the STA can receive as a beamformee in an SU PPDU using a beamforming steering matrix derived from a VHT Compressed Beamforming report with Feedback Type subfield indicating MU in the corresponding VHT Compressed Beamforming frame sent by the STA. Set to 0 for $N_{SS} = 1$ Set to 1 for $N_{SS} = 2$ ... Set to 7 for $N_{SS} = 8$
Rx NSS Type	Set to 0 to indicate that the Rx NSS subfield carries the maximum number of spatial streams that the STA can receive. Set to 1 to indicate that the Rx NSS subfield carries the maximum number of spatial streams that the STA can receive in an SU PPDU using a beamforming steering matrix derived from a VHT Compressed Beamforming report with the Feedback Type subfield indicating MU in the corresponding VHT Compressed Beamforming frame sent by the STA. NOTE—An AP always sets this field to 0.

图5

其中Rx Nss Type=0，Rx Nss=1表示终端支持接收的最大空间流数为2。

802.11协议对VHT Capabilities Info field中的Supported VHT-MCS and NSS Set subfields规定如下（图6、图7）：

Table 8-183w—Supported VHT-MCS and NSS Set subfields

Subfield	Definition	Encoding
Rx VHT-MCS Map	Indicates the maximum value of the RXVECTOR parameter MCS of a PPDU that can be received at all channel widths supported by this STA for each number of spatial streams.	The format and encoding of this subfield are defined in Figure 8-401bs and the associated description.

图6

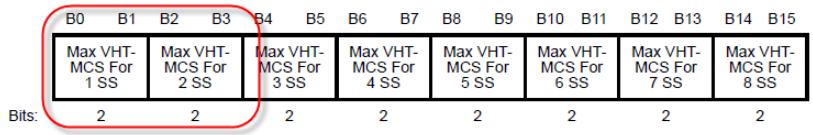

Figure 8-401bs—Rx VHT-MCS Map and Tx VHT-MCS Map subfields and Basic VHT-MCS and NSS Set field

The Max VHT-MCS For *n* SS subfield (where *n* = 1, ..., 8) is encoded as follows:

- 0 indicates support for VHT-MCS 0-7 for *n* spatial streams
- 1 indicates support for VHT-MCS 0-8 for *n* spatial streams
- 2 indicates support for VHT-MCS 0-9 for *n* spatial streams
- 3 indicates that *n* spatial streams is not supported

图7

此处可以理解为，如果终端支持该空间流数，则标记0~2，指示该空间流支持的速率集的索引。如果终端不支持该空间流，则标记位3（0x11），表示不支持。

根据现象，继续研究发现：

三星S7与H3C 5320关联请求报文中

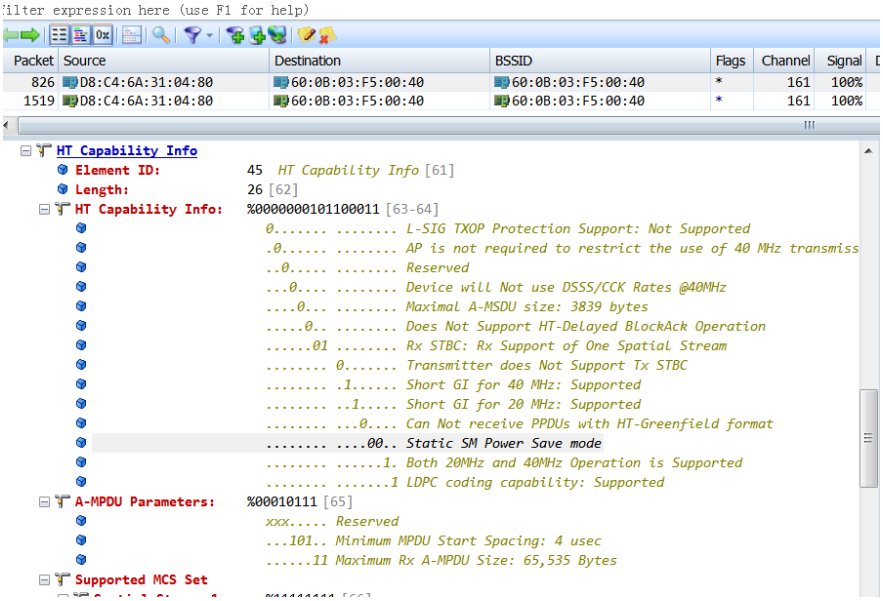

图8

在HT Capability Info中将Static SM Power Save置00表示开启power save模式，这样会使用单流模式进行关联，目的为了节省消耗。

三星S7与CISCO AP关联请求报文

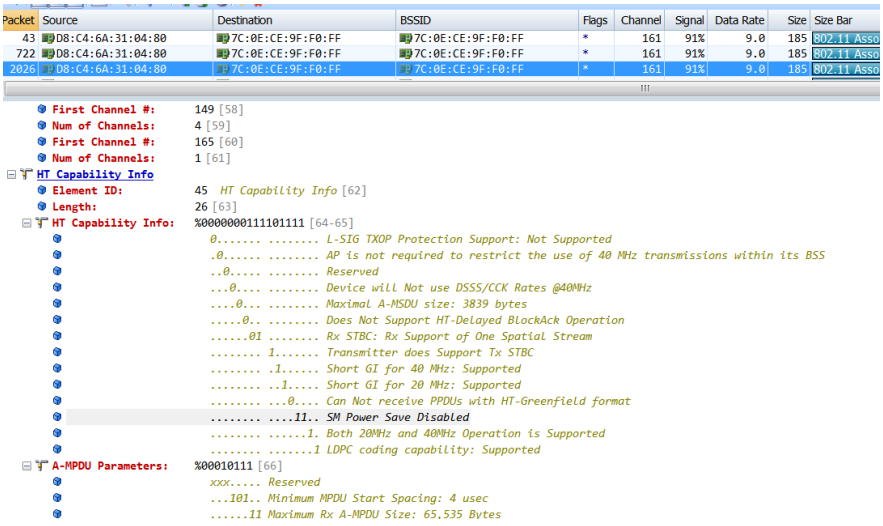

图9

在HT Capability Info中将Static SM Power Save置11表示关闭power save模式，这样会使用单流模式进行关联。

最终原因：

由于AP5320及AP5620支持mu-mimo的特性，三星S7手机会根据VHT里面的MU的能力集来决定协商的流数和SM休眠模式；当mu-mimo使能的情况下，三星S7手机在关联请求报文中会置位Static休眠标记（这个会影响后面的MIMO空间流数量），以及opertation mode参数，此时协商成单流。

关闭mu-mimo需要使用命令[H3C-wlan-ap-5320-radio-1] mu-txbf disable，这样就能协商成双流模式；而之前通过AP隐藏命令去操作只是修改了AP的驱动参数，但是AP并不参与beacon的发送，beacon还是由AC发起的，在发送出去的beacon中还是携带了mu-mimo的信息，因此终端会主动power save并且关闭一条流进行协商。这个估计是三星S7认为MU-mimo的特性下，为了更好的用MU-MIMO，所以直接以单条流工作，既节能又直接用MU-MIMO。

四、解决方法

在AC上关闭AP的mu-mimo功能；[H3C-wlan-ap-5320-radio-1] mu-txbf disable。