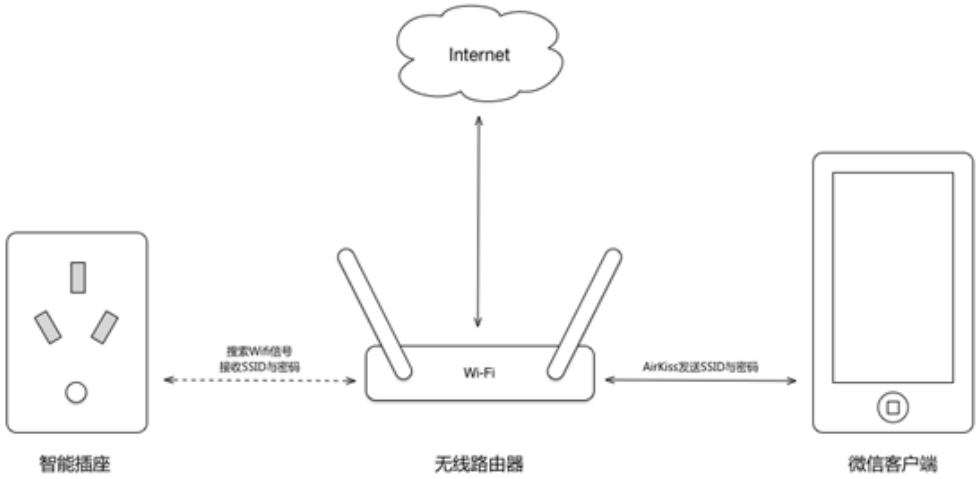
RK 平台_RTL8723DS_AIRKISS 配网说明

原理介绍



这里有 3 个节点：

智能设备：抓取路由器发出的包

路由器：转发收到的手机发出来的包

手机：发送广播包到路由器

通过上图可以看到我们的设备是通过抓取路由器转发手机的包来实现获取 SSID 和密码的。

关键点：智能设备必须能够抓到路由器的包，否则配网肯定会失败；

首先介绍下空中包分类，如下表：

包有 protocol、frequency、MIMO（几 x 几的意思，1MIMO 表示 1x1 2MIMO 表示 2x2 4MIMO 表示 4x4）差别

Wi-Fi使用的radio frequency頻段為2.4GHz或者5GHz，簡單整理成下表：

Protocol	Frequency	Max PHY Rate	Inside	Outside
Legacy	2.4–2.5GHz	2Mbps	–	–
802.11a	5.15–5.35GHz 5.47– 5.725GHz 5.725– 5.875GHz	54Mbps	30m	45m
802.11b	2.4–2.5GHz	11Mbps	30m	100m
802.11g	2.4–2.5GHz	54Mbps	30m	100m
802.11n	2.4 / 5GHz	150Mbps(40MHz * 1MIMO)	70m	250m
		600Mbps(40MHz * 4MIMO)		
802.11ac	5GHz	200Mbps(40MHz * 1MIMO) 433.3Mbps(80MHz * 1MIMO) 866.7Mbps(160MHz * 1MIMO)	35m	

RTL8723DS 单根天线（1MIMO 1X1），并且是 11 b/g/n 的模块，不支持 5G，也不支持 11ac，最大支持 11n 150Mbps(**如上图的红色方框**)。

由于以上原因，如果满足以下几个条件都是有"可能"会造成 RTL8723DS 收不到路由器发过来的包。(**注 AP 都是指代路由器**)：

- 手机和 AP 都是双天线(2x2)：因为 RTL8723DS 是单天线模组，无法解析 MIMO（2x2）的包；
- 手机和 AP 都跑在 5GHz：因为 RTL8723DS 是 2.4GHz only 模块，无法解析 5GHz 的包；
- 手机和 AP 都支持 11AC：因为 RTL8723DS 只支持到 11n，无法解析 11ac 的包；
- AP 路由器不转发手机的包或者只转发很少部分的包，导致配网失败；
- 环境干扰，配网非常依赖路由器转发的包，所以当前环境干扰非常大时，会概率出现配网失败
- 有些路由器是 LDPC 编码的，RTL8723DS 无法接收；

当以上任一条件满足时，都可能会出现无法用 airkiss 进行配网的情况。

例外情况：有时发现当满足上面某一条件时"可能也会成功"的原因是：

1、 虽然手机发出來的 2x2/11ac 的包无法解析，但 AP 有可能会用 11bgn 的速率来转发，注意不是每个 AP 都会做这样转发的动作（像**部分**小米、tplink 路由器都会有不转发或者转发少的问题）。所以如果 AP 有用 bgn 速率转发的话，仍然有"可能"可以进行配网。

2、 当设备离 AP 比较远或者干扰比较大，会导致信号传到设备这边时比较弱，包的速率衰减为 bgn 的速率的话，也有"可能"配网成功。

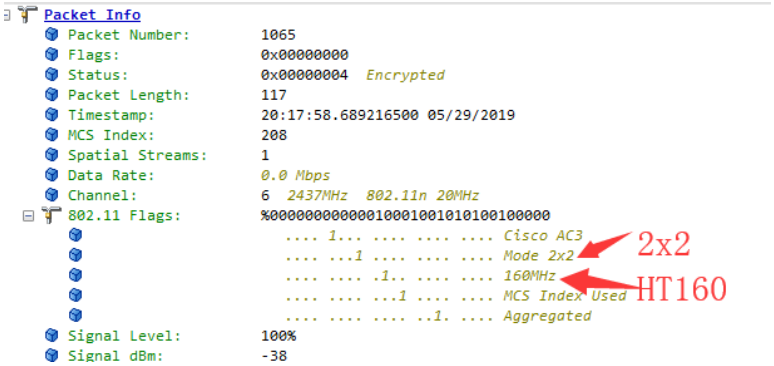
测试发现：iPhone7 及其以上型号的手机以及最近两年上市的各品牌 android 旗舰机基本都是 2x2 + 11ac 的， 只能依靠路由器转发且以较低 bgn 速率发出来的包进行配网，所以整体看来 airkiss 配网有诸多限制且成功率不是太高。

所以使用 airkiss 配网，通常都会有一个 backup solution 来支持，也就是说当无法配网时可以启用：SOFTAP/BLE 方法来弥补这样的问题，有界面的直接做类似手机的配网方法。

下面介绍如何判断配网异常是否属于哪一种情况：

需要专门抓包工具进行分析，下面的例子都是用抓包工具抓取的包

- **包是 2x2 导致的失败**



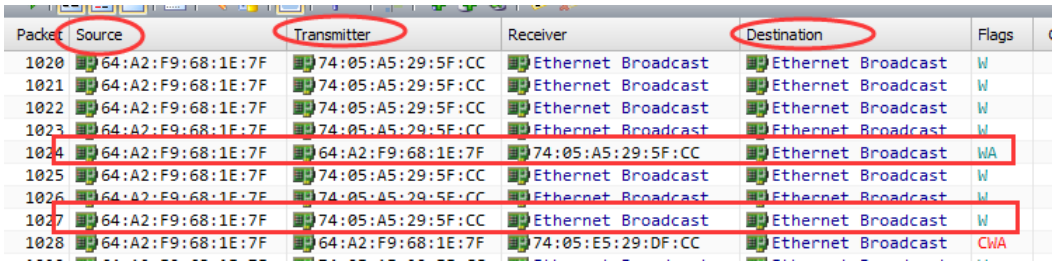
- **包是 11ac 导致的失败**

路由器转发问题

手机 mac 地址是 64 开头，路由器 mac 地址是 74 开头，路由器转发的包有个标志：transmitter 都是路由器的 mac 地址，

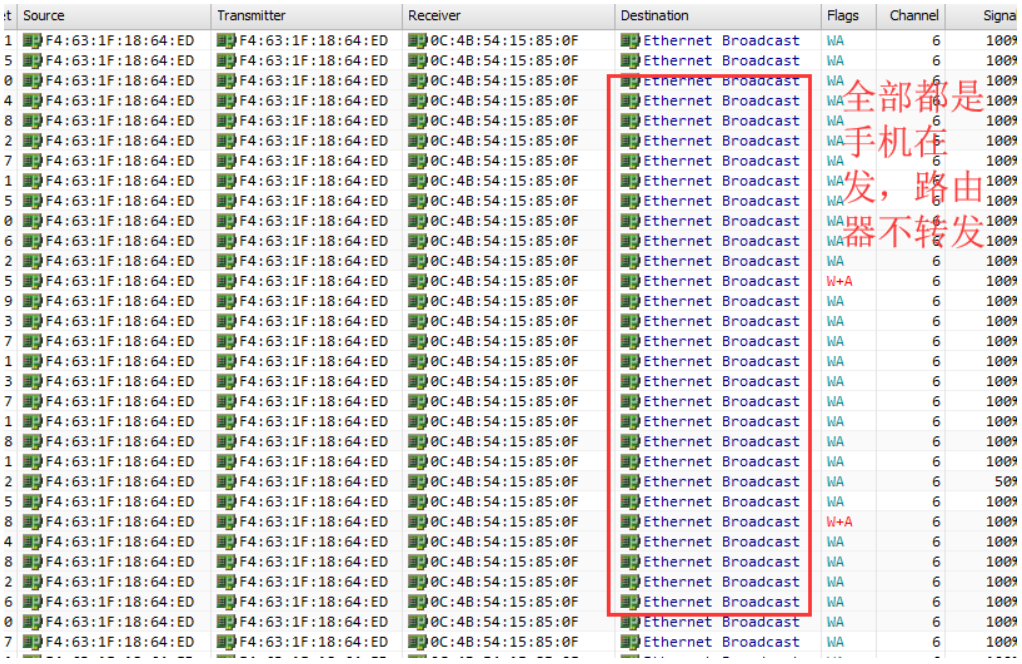
上面红色方框是手机发出来的；

下面红色方框是路由器发出来的，如果抓包没有发现，则表示路由器没做转发；



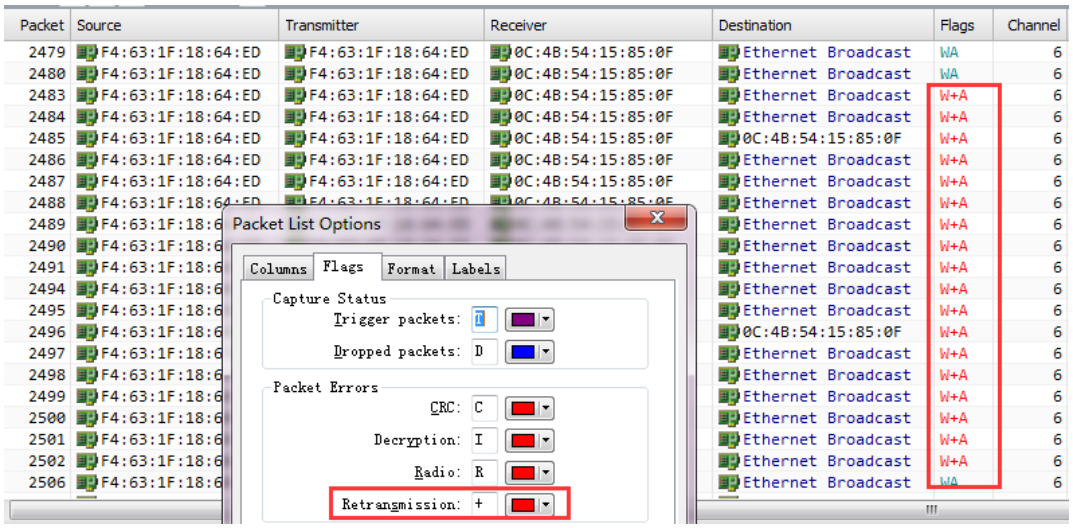
Packet	Source	Transmitter	Receiver	Destination	Flags
1020	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1021	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1022	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1023	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1024	64:A2:F9:68:1E:7F	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	WA
1025	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1026	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1027	64:A2:F9:68:1E:7F	74:05:A5:29:5F:CC	Ethernet Broadcast	Ethernet Broadcast	W
1028	74:05:E5:29:DF:CC	64:A2:F9:68:1E:7F	74:05:E5:29:DF:CC	Ethernet Broadcast	CWA

- **手机一直在发，路由器不转发导致的失败**

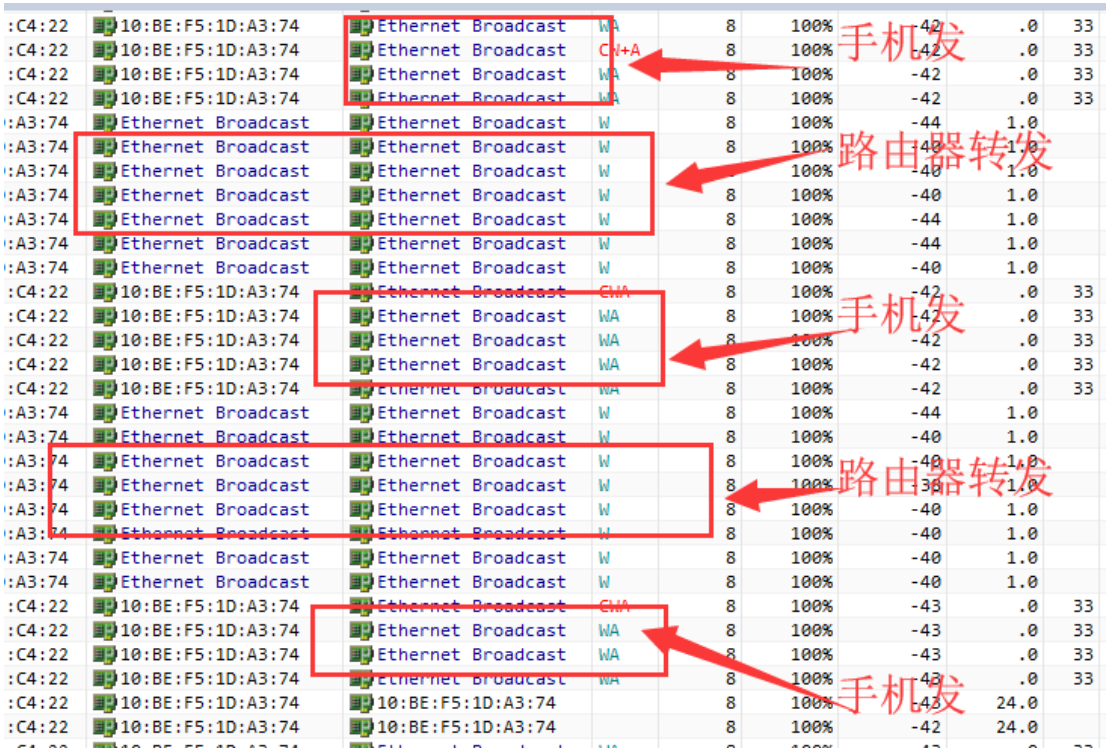


	Source	Transmitter	Receiver	Destination	Flags	Channel	Signa
1	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
5	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
0	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
4	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
8	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
2	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
7	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
1	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
5	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
0	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
6	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
2	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
5	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	W+A	6	1009
9	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
3	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
7	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
1	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
3	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
7	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
1	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
8	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
1	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
2	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	509
5	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
8	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	W+A	6	1009
4	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
8	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
2	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
6	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
0	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009
7	F4:63:1F:18:64:ED	F4:63:1F:18:64:ED	0C:4B:54:15:85:0F	Ethernet Broadcast	WA	6	1009

- **环境干扰严重导致的失败（可以看到有非常多重传帧）**



正常情况是手机和路由器间隔发，即路由器收到手机的包后马上转发出去



◆ 包是 LDPC 编码的导致失败

```
QBSS:     ID=11 Len=5 Station Count=2 Channel Utilization=83 Avail Admission Capacity=0 [104-110]
HT Capability Info
    Element ID:            45  HT Capability Info [111]
    Length:                26 [112]
  HT Capability Info:      %0001100110101101 [113-114]
                           0....... ........ L-SIG TXOP Protection Support: Not Supported
                           .0...... ........ AP does Not allow use of 40MHz Transmissions In Neighboring BSSs
                           ..0..... ........ Reserved
                           ...1.... ........ BSS does Allow use of DSSS/CCK Rates @40MHz
                           ....1... ........ Maximal A-MSDU size: 7935 bytes
                           .....0.. ........ Does Not Support HT-Delayed BlockAck Operation
                           ......01 ........ Rx STBC: Rx Support of One Spatial Stream
                           ........ 1....... Transmitter does Support Tx STBC
                           ........ .0...... Short GI for 40 MHz: Not Supported
                           ........ ..1..... Short GI for 20 MHz: Supported
                           ........ ...0.... Can Not receive PPDUs with HT-Greenfield format
                           ........ ....11.. SM Power Save Disabled
                           ........ ......0. Only 20MHz Operation is Supported
                           ........ .......1 LDPC coding capability: Supported
  A-MPDU Parameters:       %00010111 [115]
```